ROUTING IN WIRELESS SENSOR NETWORKS

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science & Engineering

By:
Gaurav Sharma
(80732005)

Under the supervision of:
Dr. A. K. Verma
Assistant Professor
&
Mr. Vinod Bhalla
Sr. Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

MAY 2009

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Routing in Wireless Sensor Networks"**, in partial fulfilment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. A. K. Verma* and *Mr. V. K. Bhalla* and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(Gaurav Sharma)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(**Dr. A. K. Verma)**
Assistant Professor
Computer Science & Engineering Department
Thapar University
Patiala.

(Mr. V. K. Bhalla)
Sr. Lecturer
Computer Science and Engineering Department
Thapar University
Patiala.

Countersigned by:

(Rajesh Bhatia)
Head
Computer Science & Engineering Department,
Thapar University,
Patiala.

(R. K. Sharma)
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

No volume of words is enough to express my gratitude towards my guides, ***Dr. Anil Kumar Verma****, Assistant Professor and* ***Mr. Vinod Kumar Bhalla****, Sr. Lecturer, Computer Science and Engineering Department, Thapar University, who have been very concerned and have aided for all the material essential for the preparation of this thesis report. They have helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research-oriented venture.*

I am also thankful to ***Dr. Rajesh Bhatia****, Head of Department, CSED,* ***Dr. Seema Bawa,****Professor,* ***Dr. Inderveer Channa****, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.*

I am also thankful to my brother ***Himanshu,*** *my sister* ***Anu,*** *and my friends* ***Anshu, Arindam, Paritosh, Suman*** *and PhD scholar* ***Shashi.***

I also thankful to ***Elmurod A. Talipov,*** *S. Korea, for providing me help and support.*

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my ***Parents*** *and the* ***Almighty*** *for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.*

Gaurav Sharma

80732005

Abstract

Wireless Sensor Networks (WSNs) consist of thousands of tiny nodes having the capability of sensing, computation, and wireless communications. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy consumption is an essential design issues. Since wireless sensor network protocols are application specific, so the focus has been given to the routing protocols that might differ depending on the application and network architecture. The study of various routing protocols for sensor networks presents a classification for the various approaches pursued. The three main categories explored are data-centric, hierarchical and location-based. Each of the routing schemes and algorithms has the common objective of trying to get better throughput and to extend the lifetime of the sensor network.

A comparison has been made between two routing protocols, Flooding and Directed Diffusion, on the basis of throughput and lifetime of the network. Simulation of AODV (WPAN) is also carried over two topologies with same source and destination node.

Keywords: Wireless Sensor Networks, Flooding, Directed Diffusion, AODV.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACK	Acknowledgement
ADC	Analog to Digital Convertor
AI	Artificial Intelligence
AODV	Ad-hoc On-demand Distance Vector
BE	Backoff Exponent
BP	Backoff Period
CAP	Contention Access Period
CBR	Continuous Bit Rate
CCA	Clear Channel Assessment
CFP	Contention Free Period
CRC	Cyclic Redundancy Check
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA-CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear-To-Send message
DARPA	Defence Advanced Research Project Agency
DSN	Distributed Sensor Networks
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
FC4	Fedora Core 4
FTP	File Transfer Protocol
GPS	Global Positioning System
GTS	Guaranteed Time Slot
GUI	Graphical User Interface I
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPTO	Information Processing Techniques Office
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LQI	Link Quality Indication
LR-WPAN	Low Rate Wireless Personal Area Network

MAC	Medium Access Control
MAN	Metropolitan Area Network
MEMS	Micro-Electro-Mechanical System
NAM	Network Animation
NB	Number of Backoffs
NS	Network Simulator
OTcl	Object Oriented Tool Command Language
PAN	Personal Area Network
PDAs	Personal Digital Assistants
PHY	PHYsical
QoS	Quality of Service
RREP	Route REPly
RREQ	Route REQuest
RTS	Ready-To-Send message
SensIT	Sensor Information Technology
SOSUS	SOund SUrveillance System
SSCS	Service Specific Convergence Sub-layer
Tcl	Tool Command Language
TCP/IP	Transmission Control Protocol/Internet Protocol
Tx	Transmission
UDP	User Datagram Protocol
VINT	Virtual InterNetwork Test-bed
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Senor Network

CHAPTER 1

INTRODUCTION

1.1. Motivation

The popularity of laptops, cell phones, PDAs, GPS devices, RFID, and intelligent computing devices is increasing day-by-day. This made the things cheaper, more mobile, more distributed, and more pervasive in daily life. Now, it is possible to construct a wallet size embedded system with the equivalent capability of a PC. Such embedded systems can be supported with scaled down Windows or Linux operating systems. In this scenario, the emergence of wireless sensor networks (WSNs) is essentially toward the miniaturization and ubiquity of computing devices. Sensor networks are composed of thousands of resource constrained sensor nodes and also some resourced base stations are there. All nodes in a network communicate with each other via wireless communication. Moreover, the energy required to transmit a message is about twice as great as the energy needed to receive the same message. The route of each message destined to the base station is really crucial in terms network lifetime: e.g., using short routes to the base station that contains nodes with depleted batteries may yield decreased network lifetime. On the other hand, using a long route composed of many sensor nodes can significantly increase the network delay.

But, some requirements for the routing protocols are conflicting. Always selecting the shortest route towards the base station causes the intermediate nodes to deplete faster, this results in a decreased network lifetime. At the same time, always choosing the shortest path might result in lowest energy consumption and lowest network delay. Finally, the routing objectives are tailored by the application; e.g., real-time applications require minimal network delay, while applications performing statistical computations may require maximized network lifetime. Hence, different routing mechanisms have been proposed for different applications. These routing mechanisms primarily differ in terms of routing objectives and routing techniques, where the techniques are mainly influenced by the network characteristics.

1.2. State of the Art

Typically, a wireless sensor node has the capability of sensing, computing, communication. The components of sensor node 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. A WSN usually consists of tens to thousands of such nodes that communicate through wireless channels for information sharing and cooperative processing. In a typical scenario, users can retrieve information of interest from a WSN by injecting queries and gathering results from the base stations or sink nodes, which behave as an interface between users and the network. In this way, WSNs can be considered as a distributed database. The sensor networks will ultimately be connected to the Internet, through which global information sharing becomes feasible.

1.3. Thesis Outline

We have organized the thesis into 7 chapters which include Introduction; Background Information; Literature Review; Problem Statement; Installation, Simulation and Design; Results, Performance Evaluation and Analysis and finally Conclusion and Future Scope.

Chapter 1 describes Wireless Sensor Network in general in terms of motivation and then follows by state of art and finally the whole thesis outline. Chapter 2, we discuss the background information relating to WSN and it's routing. Chapter 3, we study the state of the art of various routing protocols in WSN. Flooding, Directed Diffusion and AODV protocol in detail has been discussed covering the description of protocol modes and working, structure of various packets being transferred; procedures followed by the nodes in the particular modes. We also discussed Wireless Network standards and the concept of CSMA-CA. Chapter 4 discusses the problem statement and tasks. Chapter 5 discusses the installation of tools and the simulation environment. Chapter 6 describes the results, evaluates the performance, and analysis and finally Chapter 7 summarizes the conclusions drawn in the thesis along with future research directions.

CHAPTER 2

BACKGROUND INFORMATION

2.1. Wireless Sensor Networks

Wireless Sensor Networks consists of individual nodes that are able to interact with their environment by sensing or controlling physical parameter; these nodes have to collaborate in order to fulfil their tasks as usually, a single node is incapable of doing so; and they use wireless communication to enable this collaboration [1]. The definition of WSN, according to, SmartDust program of DARPA is:

"A sensor network is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment" [1].

2.1.1. Evolution of Sensor Network

Sensor network development was initiated by the United States during the Cold War [2]. A network of acoustic sensors was placed at strategic locations on the bottom of the ocean to detect and track Soviet submarines. This system of acoustic sensors was called the Sound Surveillance System (SOSUS). Human operators played an important role in these systems. The sensor network was wired network that did not have the energy bandwidth constraints of wireless system.

Modern research on sensor networks started around 1980 with the Distributed Sensor Networks (DSN) program at the Defence Advanced Research Projects Agency (DARPA). These included acoustic sensors communication (a high-level protocols that link processes working on a common application in a resource-sharing network), processing techniques, algorithms (including self-location algorithms for sensors), and distributed software (dynamically modifiable distributed systems and language design).

Recent advances in computing and communication have caused a significant shift in sensor network research and brought it closer to achieving the original vision. Small and inexpensive sensors based upon micro-electro-mechanical system (MEMS)

technology, wireless networking, and inexpensive low-power processors allow the deployment of wireless ad hoc networks for various applications. Thus, the program developed with new networking techniques is suitable for highly dynamic *ad hoc* environments.

Table 2.1. Evolution of Sensor Node [2]

	1980's-1990's	2000-2009	2010
Manufacturer	Custom contractors	Commercial: Crossbow Technology Inc., Sensoria Corp., Ember Corp.	Dust Inc. and others
Size	Large shoe box and up	Pack of cards to small shoe box	Dust particles
Weight	Kilograms	Grams	Negligible
Node Architecture	Separate sensing, processing and communication	Integrated sensing, processing and communication	Integrated sensing, processing and communication
Topology	Point-to-point, star	Client-server, peer-to-peer	Peer-to-peer
Power Supply Lifetime	Large batteries; hours days and longer	AA batteries; days to weeks	Solar; months to years
Deployment	Vehicle-placed on air-dropped single sensors	Hand-placed	Embedded, sprinkled, left behind

Wireless networks based upon IEEE 802.11 standards [10] can now provide bandwidth approaching those of wired networks. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer.

The organization has defined the IEEE 802.15 standard [15] for personal area networks (PANs), with "personal networks" defined to have a radius of 5 to 10 m. Networks of short-range sensors are the ideal technology to be employed in PANs. Furthermore, increases in chip capacity and processor production capabilities have reduced the energy per bit requirement for both computing and communication. Sensing, computing, and communications can now be performed on a single chip, further reducing the cost and allowing deployment in ever-larger numbers.

2.1.2. Wireless Sensor Network Model

Unlike their ancestor ad-hoc networks, WSNs are resource limited, they are deployed densely, they are prone to failures, the number of nodes in WSNs is several orders higher than that of ad hoc networks, WSN network topology is constantly changing, WSNs use broadcast communication mediums and finally sensor nodes don't have a global identification tags [3]. The major components of a typical sensor network are:

- *Sensor Field:* A sensor field can be considered as the area in which the nodes are placed.
- *Sensor Nodes:* Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink.
- *Sink:* A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. Sinks are also known as data aggregation points.
- *Task Manager:* The task manager also known as base station is a centralised point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing and storage centre and an access point for a human interface. The base station is either a laptop or a workstation.

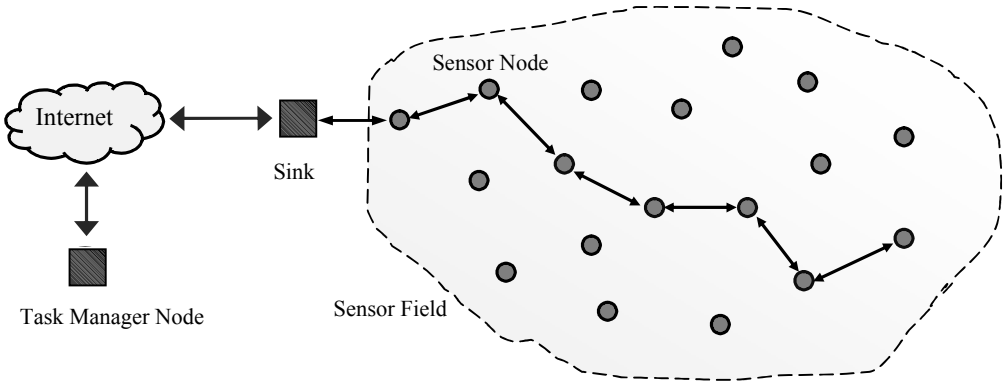


Fig. 2.1. Components of Wireless Sensor Networks

Data is streamed to these workstations either via the internet, wireless channels, satellite etc. So, hundreds to several thousand nodes are deployed throughout a sensor field to create a wireless multi-hop network. Nodes can use wireless

communication media such as infrared, radio, optical media or Bluetooth for their communications. The transmission range of the nodes varies according to the communication protocol is used.

2.1.3. The Sensor Node

A sensor is a small device that has a micro-sensor technology, low power signal processing, low power computation and a short-range communications capability. Sensor nodes are conventionally made up of four basic components as shown in Figure 2.2: a sensor, a processor, a radio transceiver and a power supply/battery [3].

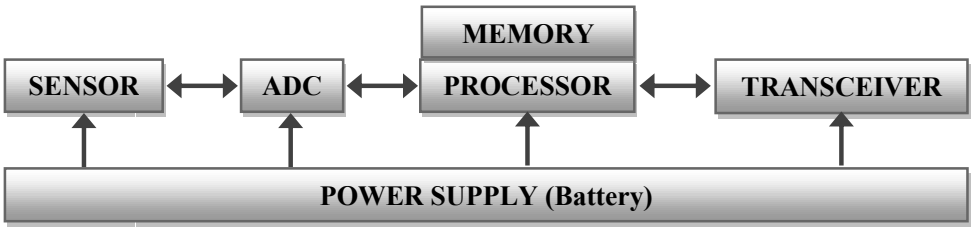


Fig.2.2. Components of a Wireless Sensor Node

Additional components may include Analog-to-Digital Convertor (ADC), location finding systems, mobilizers that are required to move the node in specific applications and power generators. The analog signals are measured by the sensors are digitized via an ADC and in turn fed into the processor. The processor and its associated memory commonly RAM is used to manage the procedures that make the sensor node carry out its assigned sensing and collaboration tasks. The radio transceiver connects the node with the network and serves as the communication medium of the node. Memories like EEPROM or flash are used to store the program code. The power supply/battery is the most important component of the sensor node because it implicitly determines the lifetime of the entire network. Due to size limitations of AA batteries or quartz, cells are used as the primary sources of power. To give an indication of the energy consumption involved, the average sensor node will expend approximately 4.8mA receiving a message, 12mA transmits a packet and 5μA sleeping [3]. In addition the CPU uses on average 5.5mA when in active mode.

2.1.4. Wireless Sensor Node Communication Architecture: Protocol Stack

The protocol stack used by the base station and sensor nodes is shown in Figure. 2.3. This protocol stack combines power and routing awareness, integrates data with

networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane and task management plane.
The physical layer should meet requirements like carrier frequency generation, frequency selection, signal detection, modulation and data encryption, transmission and receiving mechanisms.

The Data Link Layer should meet the requirements for medium access, error control, multiplexing of data streams and data frame detection. It also ensures reliable point to point and point to multi-hop connections in the network. The MAC layer in the data link layer should be capable of collision detection and use minimal power.

The network layer is responsible for routing the information received from the transport layer i.e. finding the most efficient path for the packet to travel on its way to a destination.

The Transport Layer is needed when the sensor network intends to be accessed through the internet. It helps in maintaining the flow of data whenever the application requires it.

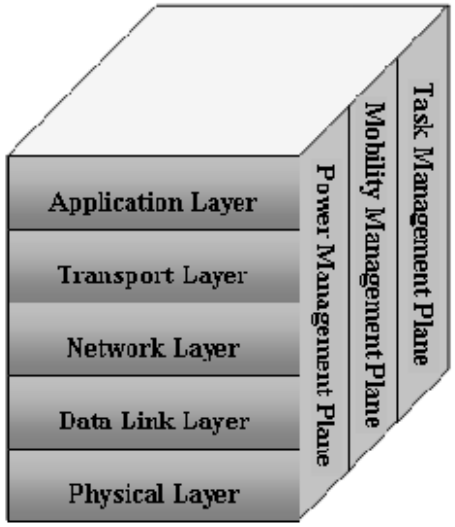


Fig. 2.3. Protocol Stack

The application layer is responsible for presenting all required information to the application and propagating requests from the application layer down to the lower

layers. The application layer software depends on the deployment and use of sensor networks.

The power management plane manages power utilization by the nodes. Mobility management plane is responsible for the movement pattern of the sensor nodes, if they are mobile. The task management plane schedules the sensing and forwarding responsibilities of the sensor nodes. Designing a network protocol for such wireless devices should meet the limitations like limited channel bandwidth, limited energy, electromagnetic wave propagation, error-prone channel, time varying conditions and mobility.

There are general ideas that can be used to overcome these limitations. Low-energy protocols help extend the limited node energy. Power control can be used to combat the radio wave attenuation. A transmitter can set the power of the radio wave, such that it will be received with an acceptable power level. Link-layer protocols and MAC protocols can be used to combat channel errors. Adaptive routing, MAC and link-layer protocols can be used to overcome the time-varying conditions of the wireless channel and node mobility.

2.1.5. Characteristics of Wireless Sensor Networks

WSNs have some unique characteristics. These are:

- Sensor nodes are small-scale devices with volumes approaching a cubic millimetre in the near future. Such small devices are very limited in the amount of energy they can store or harvest from the environment.
- Nodes are subject to failures due to depleted batteries or, more generally, due to environmental influences. Limited size and energy also typically means restricted resources (CPU performance, memory, wireless communication bandwidth and range).
- Node mobility, node failures, and environmental obstructions cause a high degree of dynamics in WSN. This includes frequent network topology changes and network partitions. Despite partitions, however, mobile nodes can transport information across partitions by physically moving between them.
- The resulting paths of information flow might have unbounded delays and are potentially unidirectional. Communication failures are also a typical problem of WSN.

- Another issue is heterogeneity. WSN may consist of a large number of rather different nodes in terms of sensors, computing power, and memory.

The large number raises scalability issues on the one hand, but provides a high level of redundancy on the other hand. Also, nodes have to operate unattended, since it is impossible to service a large number of nodes in remote, possibly inaccessible locations.

2.2. Routing in Wireless Sensor Networks

Routing is a process of determining a path between source and destination upon request of data transmission. In WSNs the network layer is mostly used to implement the routing of the incoming data. It is known that generally in multi-hop networks the source node cannot reach the sink directly. So, intermediate sensor nodes have to relay their packets. The implementation of routing tables gives the solution. These contain the lists of node option for any given packet destination. Routing table is the task of the routing algorithm along with the help of the routing protocol for their construction and maintenance.

2.2.1. Routing Challenges and Design Issues

Depending on the application, different architectures and design goals/constraints have been considered for sensor networks. Since the performance of a routing protocol is closely related to the architectural model [5].

- *Network dynamics*: Most of the network architectures assume that sensor nodes are stationary, because there are very few setups that utilize mobile sensors. It is sometimes necessary to support the mobility of sinks or cluster-heads (gateways). Route stability becomes an important optimization factor, in addition to energy, bandwidth etc. As, routing messages from or to moving nodes is more challenging. So, the sensed event can be either dynamic or static depending on the application.
- *Node deployment*: It is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths. Where as in self-organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. In later the position of the sink or the cluster-head is also crucial in terms of energy

efficiency and performance. When the distribution of nodes is not uniform, optimal clustering becomes a pressing issue to enable energy efficient network operation.

- *Energy considerations*: During the creation of an infrastructure, the process of setting up the routes is greatly influenced by energy considerations. Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi-hop routing will consume less energy than direct communication. However, multi-hop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink. Most of the time sensors are scattered randomly over an area of interest and multi-hop routing becomes unavoidable.
- *Data delivery models*: Data delivery model to the sink can be continuous, event-driven, query-driven and hybrid, depending on the application of the sensor network. In the continuous delivery model, each sensor sends data periodically. In event-driven and query-driven models, the transmission of data is triggered when an event occurs or the sink generates a query. Some networks apply a hybrid model using a combination of continuous, event-driven and query-driven data delivery. The routing protocol is highly influenced by the data delivery model, especially with regard to the minimization of energy consumption and route stability.
- *Node capabilities*: In a sensor network, different functionalities can be associated with the sensor nodes. Depending on the application a node can be dedicated to a particular special function such as relaying, sensing and aggregation since engaging the three functionalities at the same time on a node might quickly drain the energy of that node.
- *Data aggregation/fusion*: **S**imilar packets from multiple nodes can be aggregated to reduce the transmission. For this sensor nodes might generate significant redundant data. Data aggregation is the combination of data from different sources by using functions such as *suppression* (eliminating duplicates), *min, max* and *average*.

2.2.2. Routing Objectives

Some sensor network applications only require the successful delivery of messages between a source and a destination. However, there are applications that need even more assurance. These are the real-time requirements of the message delivery, and in parallel, the maximization of network lifetime.

- *Non-real time delivery*: The assurance of message delivery is indispensable for all routing protocols. It means that the protocol should always find the route between the communicating nodes, if it really exists. This correctness property can be proven in a formal way, while the average-case performance can be evaluated by measuring the message delivery ratio.
- *Real-time delivery*: Some applications require that a message must be delivered within a specified time, otherwise the message becomes useless or its information content is decreasing after the time bound. Therefore, the main objective of these protocols is to completely control the network delay. The average-case performance of these protocols can be evaluated by measuring the message delivery ratio with time constraints.
- *Network lifetime*: This protocol objective is crucial for those networks, where the application must run on sensor nodes as long as possible. The protocols aiming this concern try to balance the energy consumption equally among nodes considering their residual energy levels. However, the metric used to determine the network lifetime is also application dependent. Most protocols assume that every node is equally important and they use the time until the first node dies as a metric, or the average energy consumption of the nodes as another metric. If nodes are not equally important, then the time until the last or high-priority nodes die can be a reasonable metric.

2.2.3. Characteristics of Routing Protocols

Generally, routing protocols are : Application specific; Data centric; Capable of aggregating data; Capable of optimizing energy consumption.

2.2.4. Routing Techniques in Wireless Sensor Networks

WSN Routing Protocols can be classified in four ways, according to the way of routing paths are established, according to the network structure, according to the

protocol operation and according to the initiator of communications. Fig. 2.4 shows the classification of WSN routing protocols.

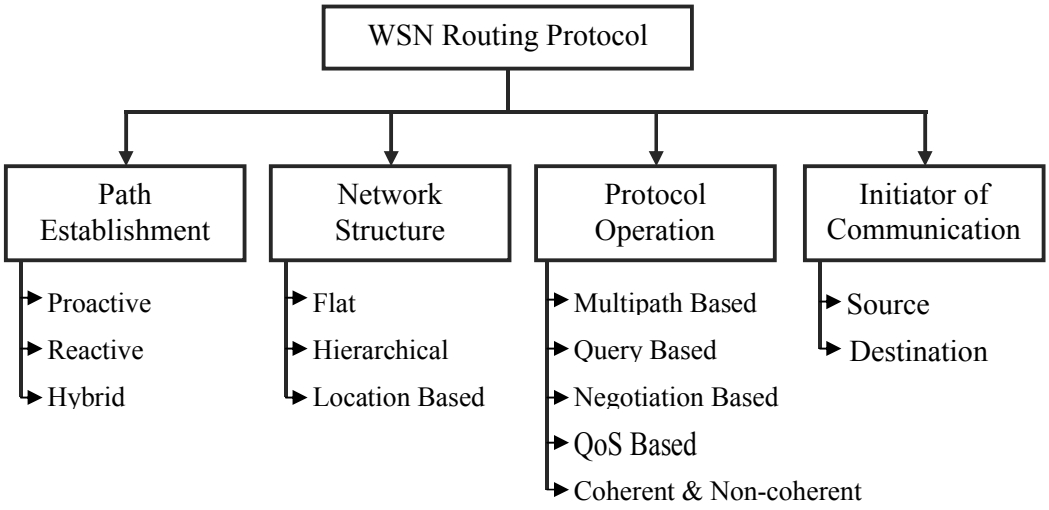


Fig. 2.4. Classification of Routing Protocols in Wireless Sensor Network.

Routing paths can be established in one of three ways, namely proactive, reactive or hybrid. Proactive protocols compute all the routes before they are really needed and then store these routes in a routing table in each node. When a route changes, the change has to be propagated throughout the network. Since a WSN could consist of thousands of nodes, the routing table that each node would have to keep could be huge and therefore proactive protocols [29] are not suited to WSNs. Reactive protocols [29] compute routes only when they are needed. Hybrid protocols use a combination of these two ideas. But in general, routing in WSNs can be divided into three categories named as flat-based routing, hierarchical-based routing and location-based routing depending on the network structure. In flat-based routing, all nodes play the same role. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation.

- *Flat Routing (Data Centric Routing protocols)* [20]: It is not feasible to assign global identifiers to each node due to the sheer number of nodes deployed in many applications of sensor networks. Such lack of global identification along with

random deployment of sensor nodes makes it hard to select a specific set of sensor nodes to be queried. Therefore, data is usually transmitted from every sensor node within the deployment region with significant redundancy. This consideration has led to data-centric routing. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions.

- *Hierarchical protocols* [26]: The major design attributes of sensor networks are scalability. Since the sensors are not capable of long-haul communication, single-gateway architecture is not scalable for a larger set of sensors. Networking clustering has been pursued in some routing approaches to cope with additional load and to be able to cover a large area of interest without degrading the service. Hierarchical routing works in two layers, first layer is used to choose cluster-heads and the other layer is used for routing. To make the WSN more energy efficient, clusters are created and special tasks (data aggregation, fusion) are assigned to them. It increases the overall system scalability, lifetime, and energy efficiency.

- *Location-based protocols* [26]: In most cases location information is needed in order to calculate the distance between two particular nodes so that energy consumption can be estimated. Generally two techniques are used to find location, one is to find the coordinate of the neighbouring node and other is to use GPS (Global Positioning System). Since, there is no addressing scheme for sensor networks like IP-addresses and they are spatially deployed on a region, location information can be utilized in routing data in an energy efficient way.

- *Multipath routing protocols* [26]: Multiple paths are used to enhance the network performance. When the primary path fails between the source and the destination an alternate path exists that measured the fault tolerance (resilience) of a protocol. This can be increased, by maintaining multiple paths between the source and the destination. This increases the cost of energy consumption and traffic generation. The alternate paths are kept alive by sending periodic messages. Due to this, network reliability can be increased. Also the overhead of maintaining the alternate paths increases.

- *Query based routing protocols* [26]: The destination nodes propagate a query for data (sensing task) from a node through the network and a node having this data

sends back the data to the node that matches the query to the query that initiates. Usually these queries are described in natural language, or in high-level query languages.

- *Negotiation based routing protocols* [26]: In order to eliminate redundant data transmissions, these use high level data descriptors through negotiation. Based on the resources that are available to them, communication decisions are taken. The motivation is that the use of flooding to disseminate data will produce implosion and overlap between the sent data; hence nodes will receive duplicate copies of the same data. This consumes more energy and more processing by sending the same data to different sensor nodes. So, the main idea of negotiation based routing in WSNs is to suppress duplicate information and prevent redundant data from being sent to the next sensor node or the base-station by conducting a series of negotiation messages before the real data transmission begins.

- *QoS-based routing protocols* [26]: In order to satisfy certain QoS (Quality of Service) metrics, e.g., delay, energy, bandwidth, etc. when delivering data to the Base Station, the network has to balance between energy consumption and data quality.

- *Coherent and non-coherent processing*: Data processing is a major component in the operation of wireless sensor networks. Hence, routing techniques employ different data processing techniques. There are two ways of data processing based routing [5].
  - *Non-coherent data processing:* In this, nodes will locally process the raw data before being sent to other nodes for further processing. The nodes that perform further processing are called the aggregators.
  - *Coherent data processing:* In coherent routing, the data is forwarded to aggregators after minimum processing. The minimum processing typically includes tasks like time stamping, duplicate suppression, etc. When all nodes are sources and send their data to the central aggregator node, a large amount of energy will be consumed and hence this process has a high cost. One way to lower the energy cost is to limit the number of sources that can send data to the central aggregator node.

CHAPTER 3

LITERATURE REVIEW

3.1. Routing Protocol

Routing is a process of determining a path between source and destination upon request of data transmission. In WSNs, the layer that is mainly used to implement the routing of the incoming data is called as network layer. When the sink is far away from the source or not in the range of source node, multi-hop technique is followed. So, intermediate sensor nodes have to relay their packets. The implementation of routing tables gives the solution. This contains the lists of node option for any given packet destination. Routing table is the task of the routing algorithm along with the help of the routing protocol for their construction and maintenance.

3.1.1. The Flooding Protocol

In flooding [6], the source node floods all events to every node in the network. Whenever a sensor receives a data message, it keeps a copy of the message and forwards the message to every one of its neighboring sensors and the cycle repeats.

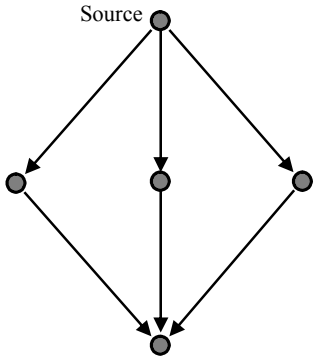


Fig. 3.1. Flooding

It is an easy-to-implement routing scheme, and it is suitable for various network types, node distributions and environments. The main advantage of flooding is the increased reliability provided by this routing method. Since the message will be sent to at least once to every host it is almost guaranteed to reach its destination. But the unlimited broadcasting the packets in the flooding scheme will cause the broadcast storm. The flooding routing protocol has three deficiencies as:

- *Implosion*: Because the nodes in the flooding scheme deliver the packets by broadcasting, the same packet may achieve the same node via different routes. When a sensor node receives a packet, it will not check the packet if it has received the packet before. This character makes the duplicated packets sent to the same place.
- *Overlap*: When these two sensors detect same event, they may both send a data of this event to the sink. This may cause that the duplicated information of an event is sent to the sink.
- *Resource blindness*: When a sensor node is not transmitting packets in flooding, it doesn't change their actives, even if the sensor nodes don't have much power to operation.

3.1.2. The Directed Diffusion Protocol

Direct Diffusion [8, 21] is the data centric protocol. It is the first proposed protocol for the wireless sensor network scenarios. If directed diffusion does not perform better than flooding, it cannot be considered viable for sensor networks. It consists of several elements: interests, data messages, gradients, and reinforcements. First, sink node requests data by sending interests. An interest message is a query or an interrogation, which specifies what a user wants to its neighbors for named data. The data is named using attribute-value pairs and it is the collected or processed information of a phenomenon that matches an interest of a user. The interests are flooded over the whole network by the sink. Such data can be an *event, which* is a short description of the sensed phenomenon. Whenever a node receives an interest, it will check whether the interest exists or new one. If it is a new interest, the sensor node will set up a gradient toward the sender to "draw" down data that matches the interest. Each pair of neighboring nodes will establish a gradient to each other. After the gradient establishment stage, the source node begins to send the related data that matches the interest to the sink. The data are generally broadcasted to all its gradient neighbors. Events are propagated toward the interest originators along multiple gradient paths. The sensor network reinforces one or a small number of these paths. The reinforcement scheme in directed diffusion is generally designed for minimum delay or maximum number of packets received during a certain period of time as shown in Figure 3.2.

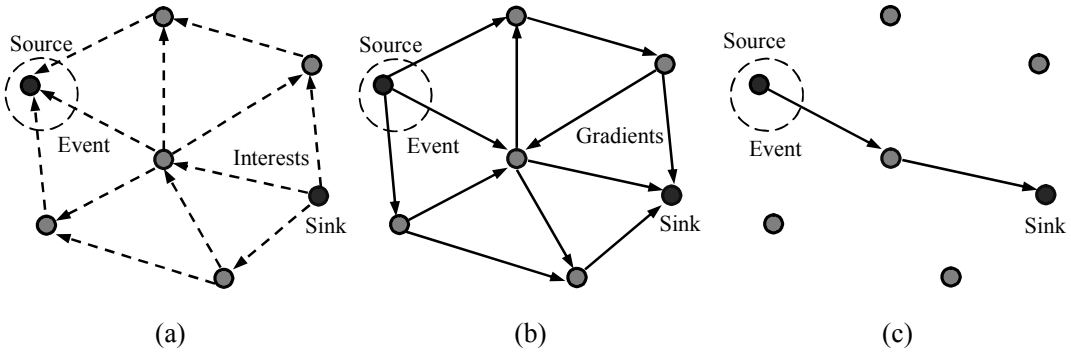


Fig. 3.2. Direct Diffusion; (a) Interest Propagation, (b) Initial gradient setup, (c) Data delivery

In directed diffusion, tasks are described or named using attribute-value pairs. For the attribute-value based naming scheme, each attribute is associated with a value range. The attribute value can be any subset of its range. There are other choices for an arrangement of attribute-value pairs and other naming schemes. To some extent, the choice of naming scheme and arrangement can affect the expressivity of tasks and may impact diffusion performance.

The interest is usually injected into the network at the sink. For each active task, the sink periodically broadcasts an interest to all its neighbours. The interval attribute specifies an event data rate. Since the location of the sources is not precisely known, interests must necessarily be diffused over a broader section of the sensor network than that covered by the potential sources. As a result, if the sink had chosen a higher initial data rate, higher energy consumption might have resulted from the wider dissemination of sensor data. The desired higher data rate can be achieved by reinforcement.

The interest is soft state, which will be periodically refreshed by the sink. Periodic interests from sinks are necessary because the interests are not reliably transmitted. To periodically refresh the interest, the sink simply re-sends the same interest with a monotonically increasing timestamp attribute. The refresh rate is a protocol design parameter that trades overhead for increased robustness to lost interests. Every node maintains an interest cache. Each item in the cache corresponds to a distinct interest. Interests do not contain information about the sink but just about the immediately previous hop. Thus, interest state scales with the number of distinct active interests. An interest entry in the cache consists of several fields. A timestamp field specifies

the timestamp of the last received matching interest. The interest entry also contains several gradient fields; up to one per neighbour. Each gradient contains a data rate field, requested by the corresponding neighbour and derived from the interval attribute of the interest and a duration field; derived from the timestamp and expires, at attributes of the interest. The duration field indicates the approximate lifetime of the gradient and the interest. Gradients are used for data propagation. For event-triggered applications, each gradient contains a gradient type instead of a data rate. There are two gradient types: an exploratory gradient and a data gradient. Exploratory gradients are intended for path setup and repair whereas data gradients are for sending real data. The default gradient type is exploratory.

When a node receives an interest, it checks if the interest exists in the cache. If no matching interest exists *i.e.,* the interest is distinct; the node creates an interest entry and determines each field of the interest entry from the received interest. This entry contains a single gradient toward the neighbour from which the interest was received, with the specified event data rate. Thus, it is necessary to distinguish individual neighbours. Any locally unique neighbour identifier like an IEEE 802.11 MAC address [10], a Bluetooth cluster address [11], a random, ephemeral transaction identifier may be applicable. If there is the matching interest entry, but no gradient for the sender of the interest, the node adds a gradient toward that neighbour and updates the timestamp and duration fields appropriately. Finally, if there are both an entry and a gradient, the node simply updates the timestamp and duration fields.

The expired gradient will be removed from its interest entry, but not all gradients will expire at the same time. For example, if two sinks send indistinct interests with different expiration times, some node in the network may have an interest entry with different gradient expiration times. When all gradients in an interest entry have expired, the interest entry is removed from a cache.

After receiving an interest, a node may decide to re-send the interest to some subset of its neighbours. To its neighbours, this interest appears to originate from the sending node, even though a distant sink might be the actual originator. With such completely local interaction, interests are diffused throughout the network. However, not all received interests are re-sent. By using the interest cache, a node may suppress a

received interest if it recently re-sent a matching interest. Generally, there are several possible choices for neighbours to re-send the interest.

The simplest alternative is to rebroadcast the interest to all neighbours, which is equivalent to flooding the interest. This alternative is reasonable in the absence of information about the sensor nodes that can satisfy the interest. Given that interests are flooded, all nodes establish gradients, as shown in Figure 3.4. Unlike the simplified description in Figure 3.2(b), every pair of neighbouring nodes establishes a gradient toward each other, as a crucial consequence of local interactions. An interest does not contain information about a sink. Therefore, when a node receives an interest, it is impossible for the node to determine whether the interest is delivered back to the node because there is a loop, the interest is delivered using another path, or the identical interest is newly generated from another sink. Such bi-directional gradients can cause a node to receive one copy of low data rate events from each of its neighbours. However, this technique can enable fast recovery from failed paths or reinforcement of empirically better paths and does not incur persistent loops.

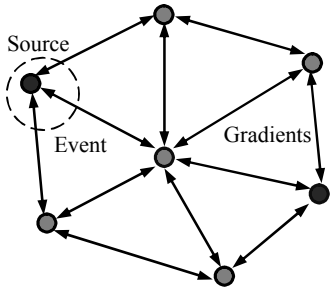


Fig. 3.3. Gradient Establishment

Generally, a gradient is composed of a *value* and a direction in which to send events. In sensor network, the gradient value is the data rate. The directed diffusion paradigm provides the designer the freedom to attach different semantics to gradient values. After a node in the specified region receives an interest, the node tasks its local sensors to collect samples to save power, sensors are off until tasked.

3.1.3. Ad-hoc On-demand Distance Vector (AODV) Protocol

AODV [12, 28] is the simplest and widely used algorithm either for wired or wireless network. It is one of the most efficient routing protocols in terms of establishing the shortest path and lowest power consumption. It is mainly used for ad-hoc networks

but also in wireless sensor networks. It uses the concepts of path discovery and maintenance. However, AODV builds routes between nodes on-demand i.e. only as needed. So, AODVs' primary objectives are:

- To broadcast discovery packets only when necessary,
- To distinguish between local connectivity management (neighbourhood detection) and general topology maintenance,
- To disseminate information about changes in local connectivity to those neighbouring mobiles nodes that are likely to need the information.

AODV does not depend on network-wide periodic advertisements of identification messages to other nodes in the network. It periodically broadcasts "HELLO" messages to the neighbouring nodes. It then uses these neighbours in routing. Whenever any node needs to send a message to some node that is not its neighbour, the source node initiates a Path Discovery, by sending a Route REQuest (RREQ) message to its neighbours. Nodes receiving the RREQ update their information about the source.

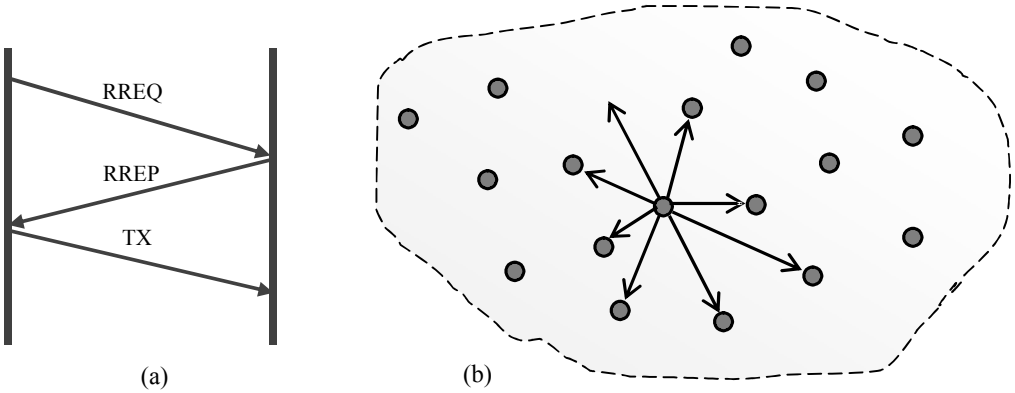


Fig. 3.4. AODV; (a) Timing diagram, (b) Broadcasts a HELLO packet to the neighbours

They also set up a backward link to the source in their routing tables. Each RREQ contains the source node's address (IP address) and a Broadcast ID that uniquely identifies it. It also has a current sequence number that determines the freshness of the message. Thus, a message number with a higher sequence number is considered to be fresher or more recent than that with a lower sequence number. The RREQ also contains a hop count variable that keeps track of the number of hops from the source. On receipt of the RREQ, the node checks whether it has already received the same RREQ earlier. If it has received the same RREQ earlier, it drops the RREQ.

Type	Reserved	Hop Count
Broadcast ID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		
Request Time		

Fig. 3.5. Structure of an RREQ packet [28]

Otherwise, if it is an intermediate node without any record of a route to the final destination, the node increases the hop count and rebroadcasts the RREQ to its neighbours. If the node is the final destination, or an intermediate node that knows the route to the final destination, it sends back the Route REPly (RREP). This RREP is sent back via the same route traversing which the node had received the message from the source.

When the source node receives the RREP, it checks whether it has an entry for the route. If it did not have any entry in its routing table, the node creates a new entry in the routing table. Otherwise it checks the sequence number of the RREP. If the RREP arrives with the same sequence number as in its tables but with a smaller hop count, or a greater sequence number (indicating fresher route), it updates its routing table and starts using this better route. Once an entry for the new route has been created in the table, the node can start communication with the destination.

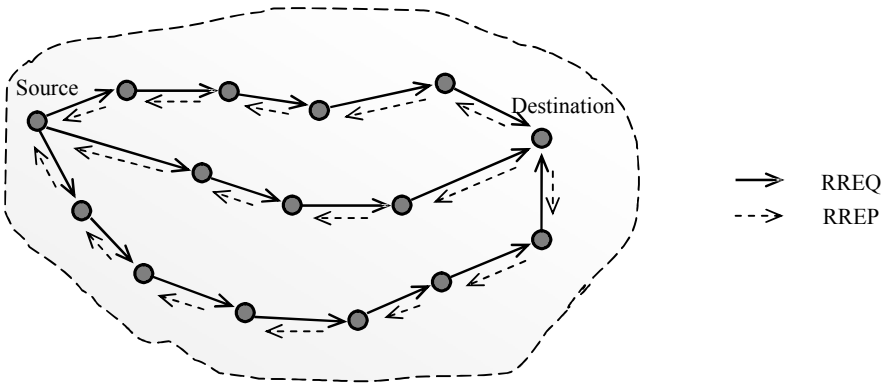


Fig. 3.6. Path Discovery of AODV

Every time a node receives subsequent RREPs, it updates its routing table information, and only forwards those that are fresher or contain a smaller hop count. Each routing table entry contains information for the destination, the next node, number of hops to the destination, sequence number for that destination, active neighbours for the route and expiration time of the table entry.

The expiration time frame is reset every time the source routes a packet to the destination. The advantage of AODV is that, it is bandwidth efficient; it has loop-free routing and acts as a reactive protocol that makes it worthy to be considered.

3.2. Wireless Networking Standards

There are various standards for wireless networking. Some of them are discussed in this section.

3.2.1. IEEE 802.11 Standard

It is a set of standards carrying out wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are implemented by the IEEE LAN/MAN Standards Committee (IEEE 802) [10]. NS2 uses Phy/WirelessPhy to simulate 802.11b wireless channel.

NS2 implements several propagation models to predict the signal power received by the receiver. The signal strength is used to determine whether the frame is transmitted successfully. These are:

- *Free Space model*: It is used to simulate path loss of wireless communication when line-of-sight path exists between transmitter and receiver.
- *Two Ray Ground model*: It is used when line-of-sight path exists and reflection of ground is considered.
- *Shadowing model*: It is used to simulate wireless channel in in-door environment.

3.2.2. IEEE 802.15 Standard

In March 1999, the IEEE established the 802.15 [14, 15] working group as part of the IEEE Computer Society's 802 Local and Metropolitan Area Standards Committee. The 802.15 working group was established with the specific purpose of developing standards for short distance wireless networks, otherwise known as wireless personal area networks (WPANs).

The IEEE 802.15.4 standard [14] defines the characteristics of the physical and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPAN). The advantages of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, use of unlicensed radio bands (ISM band), flexible and extendable networks, integrated intelligence for network set-up and message routing, and a reasonable battery life, while maintaining a simple and flexible protocol stack.

Table 3.1. IEEE Standards 802.15 [14]

PROJECT	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active devices Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.2 Coexistence	Develop a Coexistence Model and Mechanisms Document as a Recommended Practice			
802.15.3 High Rate	22, 33, 44, 55 Mbps	10M	256 active device Piconet/ Scatternet	FCC part 15.249 Qos, Fast Join Multi-Media
802.15.4 Low Rate	Up to 250 /kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer-to-Peer	Battery Life: multi-month to infinite

3.2.2.1. The Physical Layer

Physical layer of Low Rate Wireless Personal Area Network consists of 27 channel altogether. The channels available are divided in three different frequency bands: a 2450 MHz band (with 16 channels), a 915 MHz band (with 10 channels) and an 868 MHz band (1 channel), all using the Direct Sequence Spread Spectrum (DSSS) access mode. The data rates are very low compared to other types of WPAN as seen in Table 3.1.

Besides radio on/off operation, the physical layer supports functionalities for channel selection, link quality estimation, energy detection measurement and clear channel assessment to assist the channel selection. The physical layer provides an interface between the MAC sub-layer and the physical radio channel. The physical layer performs the following tasks:

- *Activation/Deactivation of radio transceiver*: Turn the radio transceiver into one of the three states, that is, transmitting, receiving, or off (sleeping) according to the request from MAC sub-layer.

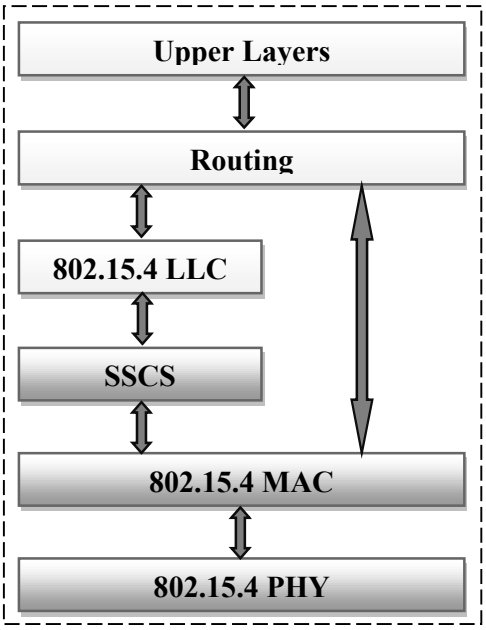


Fig. 3.7. Layer Approach of IEEE 802.15.4

- *Energy Detection (ED)*: It is an estimate of the received signal power within the bandwidth of channel. The result from energy detection can be used by a network layer as part of a channel selection algorithm, or for the purpose of clear channel assessment (CCA) (alone or combined with carrier sense).
- *Link Quality Indication (LQI)*: The measurement is performed for each received packet. The PHY layer uses receiver energy detection (ED), a signal-to-noise ratio (SNR), or a combination of these to measure the strength and/or quality of a link from which a packet is received.
- *Channel Selection*: As discussed above, the Wireless links under 802.15.4 can operate in 27 different channels but a specific network can choose to support part of the channels. Hence the PHY layer should be able to tune its transceiver into a certain channel upon receiving the request from MAC sub-layer.
- *Clear Channel Assessment (CCA) for Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)*: The PHY layer is required to perform CCA using energy detection, carrier sense, or a combination of these two. In carrier sense mode, the medium is considered busy if a signal with the modulation and spreading characteristics of IEEE 802.15.4 is detected.
- *Transmission/Reception of packets over physical medium*: Here Modulation and spreading techniques are used.

3.2.2.2. The MAC Sub-Layer

The MAC sub-layer provides an interface between the service specific convergence sub-layer (SSCS) and the PHY layer as shown in Figure.2.11. The MAC sub-layer provides two services, namely, the MAC data service and the MAC management service. It is responsible for the following tasks:

- *Generating and managing beacons*: If the device is a coordinator then the coordinator can determine whether to work in a beacon enabled mode, in which a superframe structure is used.
- *Association and disassociation with personal area network (PAN) coordinators*: To support self-configuration, 802.15.4 embeds association and disassociation functions in its MAC sub-layer. This not only enables a star to be setup automatically, but also allows for the creation of a self-configuring, peer-to-peer network.
- *Channel access*: Employing the carrier sense multiple access with collision avoidance (CSMA-CA) mechanism for channel access. Like most other protocols designed for wireless networks, 802.15.4 uses CSMA-CA mechanism for channel access. However, the new standard does not include the request-to-send (RTS) and clear-to-send (CTS) mechanism, in consideration of the low data rate used in LR-WPANs.
- *Guaranteed Time Slot management*: Handling and maintaining the guaranteed time slot (GTS) mechanism. When working in a beacon enabled mode, a coordinator can allocate portions of the active superframe to a device. These portions are called GTSs, and comprise the contention free period (CFP) of the superframe.
- *Frame validation and Acknowledged frame* delivery: It provides various mechanisms to enhance the reliability of the link between two peers, among them are the frame acknowledgment and retransmission, data verification by using a 16-bit CRC, as well as CSMA-CA.

3.2.2.3. Data Transfer Model

Data transfer [15] can happen in three different ways: (1) from a device to a coordinator; (2) from a coordinator to a device; and (3) from one peer to another in a

peer-to-peer multi-hop network. The date transfer model is also classified as direct data transmission, indirect data transmission and GTS data transmission.

Direct data transmission applies to all data transfers, either from a device to a coordinator, from a coordinator to a device, or between two peers. Un-slotted CSMA-CA or slotted CSMA-CA is used for data transmission, depending whether non-beacon enabled mode or beacon-enabled mode is used. Whereas indirect data transmission only applies to data transfer from a coordinator to its devices. Occasionally, indirect data transmission can also happen in non-beacon enabled mode. Although GTS data transmission only applies to data transfer between a device and its coordinator, either from the device to the coordinator or from the coordinator to the device. No CSMA-CA is needed in GTS data transmission.

3.3. Carrier Sense Multiple Access – Collision Avoidance

When two nodes want to send data at the same time, CSMA-CA [16, 17] comes into play. It gives the solution of hidden node problem in CSMA-CD, in which a node cannot detect another node that also wants to transmit packet resulting a collision. CSMA-CA protocol uses four-way handshake.

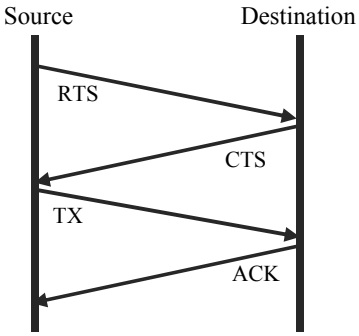


Fig. 3.8. Timing diagram for CSMA-CA

The node will listen (sense a voltage level) before transmit any packet. If it detects there is a signal, it will waits for a random period before listens to the network again. If no signal is detected, the node will send ready-to-send message (RTS) to all nodes. The RTS contains destination address and period of the transmission. The destination will reply with clear-to-send message (CTS) that denotes that the node can send message without collision. The destination/receiver will send acknowledgement for every packet it received. If ACK is not received, the packet is assumed lost or

corrupted and will resend the packet until ACK is received. The IEEE 802.15.4 uses two types of channel access mechanism, depending on the network configuration. Our simulation is based on Un-slotted CSMA-CA.

3.3.1. Slotted CSMA-CA

The beacon-enabled networks use this channel access mechanism, where the backoff slots are aligned with the start of the beacon transmission. Each time a device want to transmit data frame during the Contention Access Period (CAP), it shall locate the boundary of the next backoff slot and then wait for a random number of backoff slots. If the channel is busy, following this random backoff, the device shall wait for another random number backoff slots before trying to access the channel again. If the channel is idle, the device can begin transmitting on the next available backoff slot boundary.

3.3.2. Un-slotted CSMA-CA

The non-beacon-enabled networks use this channel access mechanism. If a device wants to transmit data frames or MAC commands, it will wait for a random period. If the channel is found to be idle, following the random backoff, the device shall transmit its data. If the channel is found to be busy, following the random backoff, the device will wait for another random period before trying to access the channel again. This algorithm works at Layer 2. The Un-slotted CSMA-CA is based on basic time unit called *Backoff Period* (BP). BP is equal to 0.32 ms that refer to *aUnitBackoffPeriod* (80 bits). The Un-slotted CSMA-CA backoff algorithm depends on two variables:

The Backoff Exponent (BE) enables the computation of the backoff delay, which is the time before performing Clear Channel Assessment (CCA). The backoff delay is a random variable between 0 and $(2^{BE} - 1)$.

The Number of Backoffs (NB) represents the number of times the un-slotted CSMA-CA algorithm was required to backoff while attempting to access the channel. This value is initialized to zero (NB = 0) before each new transmission attempt. First step of Un-slotted CSMA-CA is initializing NB=0 and BE=2 (depends on Battery Life Extension which is by default value is 3). Then, second step is counting down the random number of BPs that uniformly generated between 0 to $(2^{BE} - 1)$. The counting must start at the boundary of a BP. The third step is performing CCA at the boundary of the BP to access channel activity. Then, if the channel is idle, channel access is

allowed. Therefore, un-slotted CSMA-CA will be performed to send the packet. If the channel is busy, the flow will go to fourth step. The fourth step will increment NB and BE. BE can't exceed the setting maximum value.

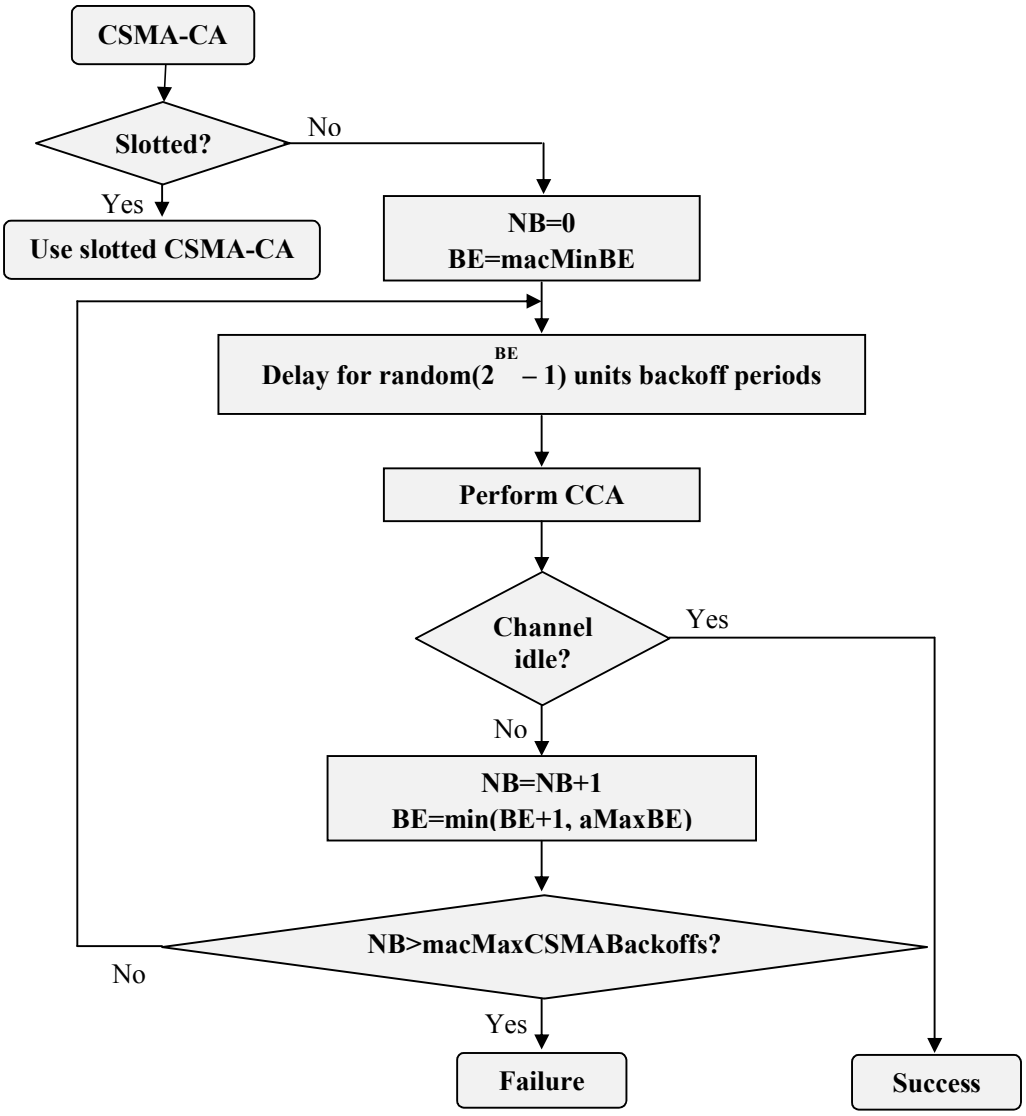


Fig. 3.9. Un-Slotted CSMA/CA Flow Chart [15]

Incrementing the BE makes the probability of backoff delays becomes big. Then, if the NB exceeds the maximum number of allowed backoffs, the transmission is fail. If NB hasn't reached the maximum value, it will repeat the second step. The un-slotted CSMA-CA will be activated each time transmission of a new packet. The same has been described in Figure 3.9.

CHAPTER 4

PROBLEM STATEMENT & OBJECTIVE

4.1. Problem Statement

Most current WSN routing protocols assume that the wireless network in benign and every node in the network strictly follow the routing behavior and is willing to forward packets to/for other nodes. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes are present in the network.

A commonly observed misbehaviour is packet dropping. Practically, in a WSN, most devices have limited computing and battery power while packet forwarding consumes a lot of such resources. The design of routing protocols for WSN's must consider the power and resource limitation of the network nodes, the time varying quality of wireless channels and possibility of packet loss and delay. To address these design requirements several design strategies for WSN's have been proposed. AODV, Flooding and directed diffusion are some of the common protocols. Each having its fair share of advantages and limitations.

The main advantage of flooding is the increased reliability provided by this routing method. Since the message will be sent at least once to every host it is almost guaranteed to reach its destination. There are several disadvantages with this approach to routing. It is very wasteful in terms of the networks total bandwidth. While a message may only have one destination it has to be sent to every host. This increases the maximum load placed upon the network. Messages can also become duplicated in the network further increasing the load on the networks bandwidth as well as requiring an increase in processing complexity to disregard duplicate messages.

Directed Diffusion uses a naming scheme for the data to save energy. The main disadvantage of directed diffusion is to use attribute-value pairs for data and queries on-demand (Interests). Interest is broadcasted by the sink to its neighbours, which can do in-network aggregation. Gradients or reply links to an interest (path establishment) are sent back to the sink. Energy saving and delay is done with caching. There is no

need for global addressing (neighbour-to-neighbour mechanism). The main disadvantage of directed diffusion is that it cannot be used for continuous data delivery (e.g., environmental monitoring) or event-driven applications. There is limited memory storage for data caching inside the sensor node. Therefore, data aggregation maybe affected.

The IEEE 802.15.4 standard defines the characteristics of the physical and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPAN). The advantages of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, use of unlicensed radio bands (ISM band), flexible and extendable networks, integrated intelligence for network set-up and message routing, and a reasonable battery life, while maintaining a simple and flexible protocol stack.

AODV expects/requires that the nodes in the broadcast medium can detect each other's broadcasts. AODV is a reactive routing protocol. This means that AODV does not discover a route until a flow is initiated. This route discovery latency result can be high in large-scale mesh networks.

4.2. Objective and Sub-tasks

In order to improve throughput in WSN, routing algorithm should be chosen carefully. The throughput of different routing protocols with different topologies has been evaluated with different simulation time. The primary objective of this thesis is to improve the throughput in WSNs which is achieved by the following manner:

- To analyze, implement and evaluate Flooding protocol.
- To analyze, implement and evaluate the directed diffusion protocol.
- A comparison is being performed between the two protocols.
- Performance of AODV protocol using WPAN is evaluated. In order to evaluate the performance of the network, the throughput with different topologies was analyzed.

CHAPTER 5

INSTALLATION, SIMULATION & DESIGN

5.1. Fedora Core 4 (8)

Fedora Core [43] is a free operating system base on Linux. Red Hat being developed by the open source community and the Red Hat engineers sponsor the development of Fedora. Fedora Core 4 (FC4) and FC8 are the release of the Fedora Project. Some primary features of FC4 are extensive performance improvements, support for Intel-based Macs and a new Graphical User Interface (GUI) virtualization manager.

5.2. The Network Simulator (NS2)

Simulation can be defined as "Imitating or estimating how events might occur in a real situation". It can involve complex mathematical modelling, role playing without the aid of technology, or combinations. The value lies in the pacing you under realistic conditions that change as a result of behaviour of others involved, so you cannot anticipate the sequence of events or the final outcome.

5.2.1. NS2 Overview

NS [45] is an event driven network simulator developed at University of California at Berkeley, USA, as a REAL network simulator projects in 1989 and was developed at with cooperation of several organizations. Now, it is a VINT project supported by DARPA. NS is not a finished tool that can manage all kinds of network model. It is actually still an on-going effort of research and development. The users are responsible to verify that their network model simulation does not contain any bugs and the community should share their discovery with all. There is a manual called NS manual for user guidance.

NS is a discrete event network simulator where the timing of events is maintained by a scheduler and able to simulate various types of network such as LAN and WPAN according to the programming scripts written by the user. Besides that, it also implements variety of applications, protocols such as TCP and UDP, network elements such as signal strength, traffic models such as FTP and CBR, router queue management mechanisms such as Drop Tail and many more.

There are two languages used in NS2 C++ and OTcl (an object oriented extension of Tcl). The compiled C++ programming hierarchy makes the simulation efficient and execution times faster. The OTcl script which written by the users the network models with their own specific topology, protocols and all requirements need. The form of output produce by the simulator also can be set using OTcl. The OTcl script is written which creating an event scheduler objects and network component object with network setup helping modules. The simulation results produce after running the scripts can be use either for simulation analysis or as an input to graphical software called Network Animation (NAM).

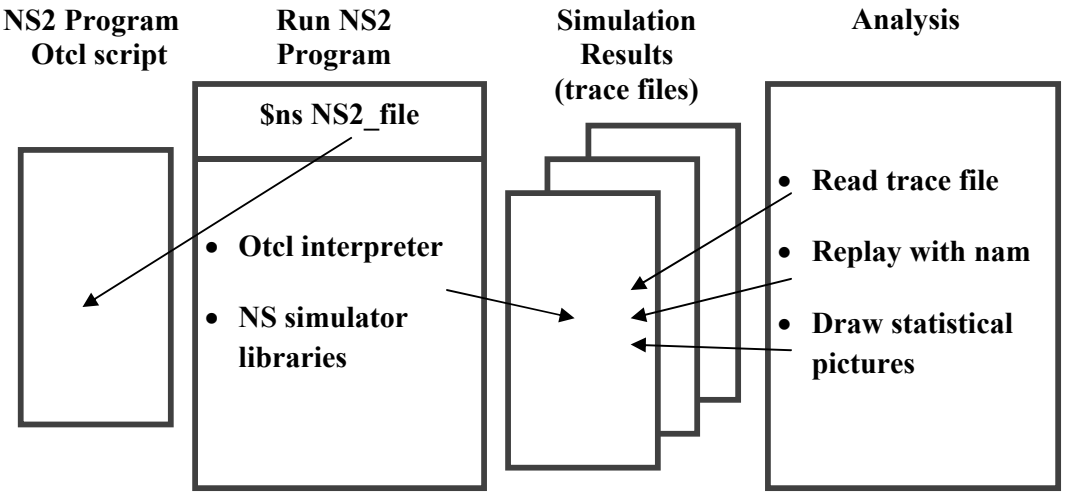


Fig. 5.1. Running NS2 Program

NS2 is an event driven network simulator, which can be implemented in Linux-based platform. This report will explain on how to install NS2 in Fedora Core platform. The NS2 files (recommended to download a piece of file which includes all the needed files called ns-allinone-2.xx from http://www.isi.edu/nsnam/ns/ must be downloaded into any media storage, most preferred is inside the computer itself where the NS2 is going to be installed. Since, we are using NS 2.29. It is not recommend logging in as a root because installation at root may interfere with any important Linux files.

5.2.2. Tool Command Language (Tcl)

Short for Tool Command Language, Tcl [46] is a powerful interpreted programming language developed by John Ouster out at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language. It has a wide range of usage,

including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs.

5.2.3. The Network Animation (NAM)

The network animator began in 1990 as a simple tool for animating packet trace data. This trace data is typically derived as output from a network simulator like ns or from real network measurements, e.g., using tcpdump. Steven McCanne wrote the original version as a member of the Network Research Group at the Lawrence Berkeley National Laboratory, and has occasionally improved the design, as he's needed it in his research. Marylou Orayani improved it further and used it for her Master's research over summer 1995 and into spring 1996. The nam development effort was an ongoing collaboration with the VINT project. Currently, it is being developed at ISI by the SAMAN and Conser projects.

5.2.4. The Trace File

The trace file is an ASCII code files and the trace is organized in 12 fields as in Figure 5.2. below.

Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addrs	Dst addrs	Seq num	Pkt id

Fig. 5.2. Fields of Trace File

The first field is the event type and given by one of four available symbols r, +, - and d which correspond respectively to receive, enqueued, dequequed and dropped. The second field is telling the time which the event occurs. The third and fourth fields are the input and output node of the link at which the events takes place. The fifth is the packet type such as continuous bit rate (cbr) or transmission control protocol (tcp). The sixth is the size of the packet and the next field is some kind of flags. The eighth field is the flow identity of IPv6, which can specify stream color of the NAM display and can be use for further analyze purposes. The ninth and tenth fields are the source and destination address in the form of “node.port”. The eleventh is the network layer protocol’s packet sequence number. NS keeps track of UDP packet sequence number for the analysis purposes. The twelfth, which is the last field, is the unique identity of

the packet. Results of simulation are stored into trace file (*.tr). Trace Graph was used to analyze the trace file.

5.2.5. The Tracegraph

It is a data presentation system for Network Simulator NS2. The simulator doesn't have any options implemented to analyse simulations results so it's hard to use it. Trace graph [47] system provides many options for analysis, including 250 graphs and statistical reports. It is implemented in MATLAB 6.0 and can be compiled to run without MATLAB. Compiled versions for Linux and Windows systems are available for download at http://www.geocities.com/tracegraph/.

Trace graph supports the following NS2 trace file formats; wired, satellite, wireless (old and new trace), wired-cum-wireless. Trace file loading stage is divided into 4 stages; automatic trace file format recognition, trace file parsing to extract necessary simulation data which is saved to a temporary file, trace files can contain much more data than is needed by the system, so unnecessary information is omitted to speed up trace file loading, temporary file loading, constants calculations (packets types, packets sizes, flows IDs, trace levels, number of nodes, simulation time) – in order to speed up data processing. Wireless and wired-cum-wireless trace files are parsed and saved in Trace graph format.

5.2.6. The Low Rate WPAN Function Modules

The LR-WPAN [14] function modules were developed by Jianliang Zheng and Myung J. Lee (2006) at The City University, New York. The work was done specially for a newly defined standard IEEE 802.15.4. They had study and developed several features such as beacon enabled mode and non-beacon enabled mode, association, tree formation and network auto-configuration, orphaning and coordination relocation, CSMA-CA for both slotted and un-slotted and direct, indirect and GTS data transmissions.

- *Wireless Scenario Definition*: It selects the routing protocol; defines the network topology; and schedules events such as initializations of PAN coordinator, coordinators and devices, and starting (stopping) applications. It defines radio-propagation model, antenna model, interface queue, traffic pattern, link error model, link and node failures, super-frame structure in beacon enabled mode, radio transmission range, and animation configuration.

- *Service Specific Convergence Sub-layer (SSCS)*: This is the interface between 802.15.4 MAC and upper layers. It provides a way to access all the MAC primitives, but it can also serve as a wrapper of those primitives for convenient operations. It is an implementation specific module and its function should be tailored to the requirements of specific applications.
- 802.15.4 PHY: It implements all 14 PHY primitives.
- 802.15.4 MAC: This is the main module. It implements all the 35 MAC sub-layer primitives.

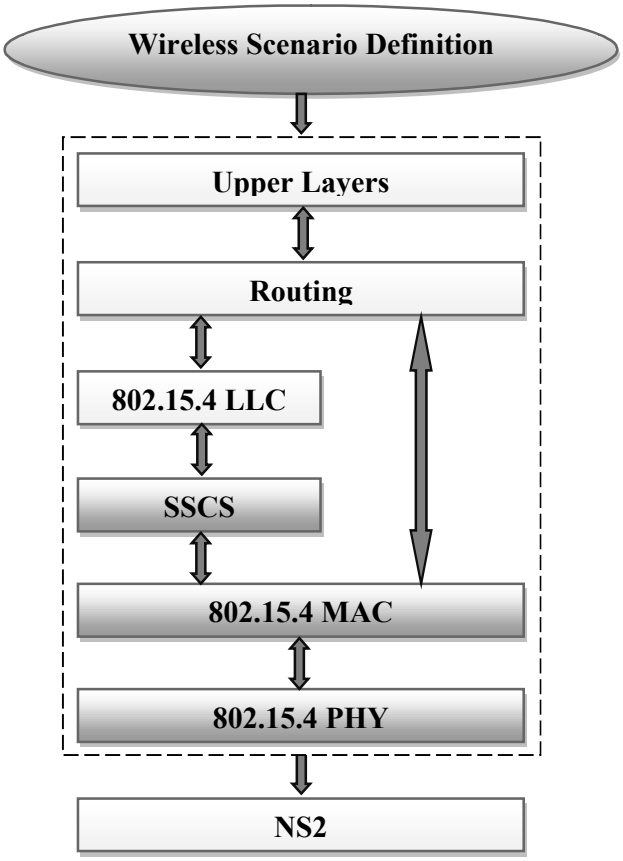


Fig. 5.3. LR-WPAN (IEEE 802.15.4) Function Modules

5.3. Simulation of Routing Protocols

Simulation of different routing protocols (Flooding, Directed Diffusion and AODV) has been carried over to evaluate the performance. Various parameters that are considered for simulation are listed in table 5.1.

Table 5.1. Network Parameter Definition

Parameter Name	Flooding	Directed Diffusion	AODV
channel type	Channel/WirelessChannel	Channel/WirelessChannel	Channel/Wireless Channel
radio model	TwoRayGround (1.559e-11)	TwoRayGround (1.559e-11)	TwoRayGround (8.54570e-07)
netif	Phy/WirelessPhy	Phy/WirelessPhy	Phy/WirelessPhy/802_15_4
mac protocol	Mac/802_11	Mac/802_11	Mac/802_15_4
ifq	Queue/DropTail/PriQueue	Queue/DropTail/PriQueue	Queue/DropTail/PriQueue
ifqlen	50	50	50
number of nodes	30	30	25
routing protocol	FLOODING	DIRECTED DIFFUSION	AODV
grid size	800 x 800	800 x 8000	50 x 50
packet size	64	64	70
simulation time	25/50/75/100 seconds	25/50/75/100 seconds	100 seconds
Topology	Random	Random	Random/Mesh
Initial energy	7 joules	7 joules	1 joule
Source Node	7	7	20
Destination node	5	5	4

CHAPTER 6

RESULTS, PERFORMANCE EVALUATION & ANALYSIS

This chapter shows the results of the simulation. The analysis is being done on the basis of the results of *.nam file and the *.tr file. We also evaluate the performance of the protocol. In the ns2-allinone package NAM is a build-in program. NAM helps us to see the flow of message between the nodes. It also shows the packets are dropping or reaching to the destination properly. When the TCL file is written, NAM is invoked inside that file. With the help of 2D and 3D graphs we have tried to analyze the simulation with different simulation time. The scripts for the NAM is stored as *.nam and for tracegraph *.tr is used. The simulation has been mainly divided in three parts that are given below:

- Simulation of flooding protocol
- Simulation of Directed Diffusion protocol
- Simulation of AODV with WPAN

The comparison between Flooding and Directed Diffusion is performed over the common factors like throughput of dropped packets, end-to-end delay and energy consumption in the network over different simulation time. Also for short-range communication, AODV with WPAN has been implemented over different topologies.

6.1. Simulation of Flooding Protocol

Simulation of flooding protocol is performed over 30 nodes having energy 7 joules. Nodes in the network are in random position. In this scenario there is a source node that will broadcast the data and all the neighbouring nodes will do the same after receiving it. Node 7 is the source node and node 5 is the sink node. In figure 6.1 source node 7 is flooding the data to its neighbouring nodes. The flooding of packets is shown by red color. Because all the nodes are flooding the data, so there will be energy loss in the network continuously. When a particular node receives a fix amount of data it changes its color to show the energy loss. In figure 6.2 some nodes became yellow due to receiving more broadcast and so more energy loss.

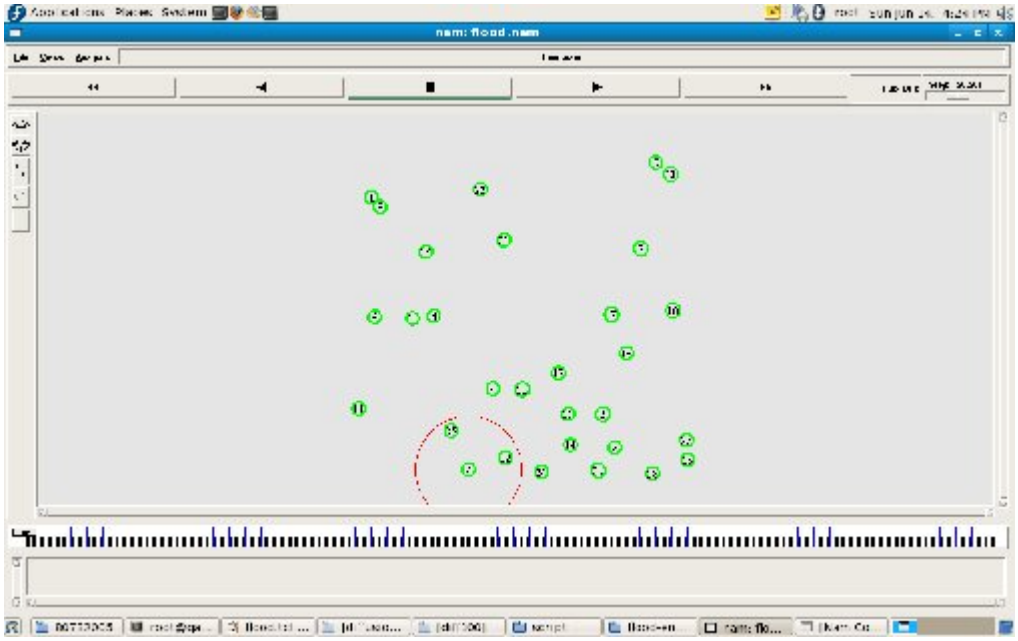


Fig. 6.1. Flooding: Node 7 Floods data

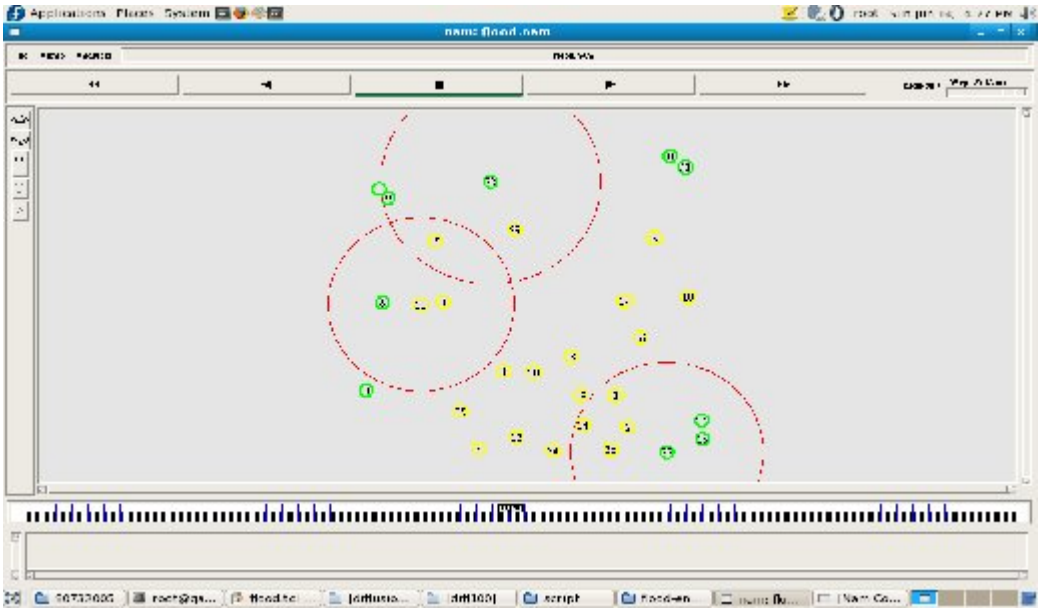


Fig. 6.2. Flooding: The nodes, receive more broadcast became yellow

In figure 6.3, all the nodes are in the critical situation and network is going to collapse. The lifetime of the network with energy 7 joule is almost 85 seconds. If energy of the network is increased, it will work for more simulation time. After the simulation time of 85 seconds sensor network is not going to send or receive any kind of message because energy of all the nodes on the path between source and sink has been diminished.

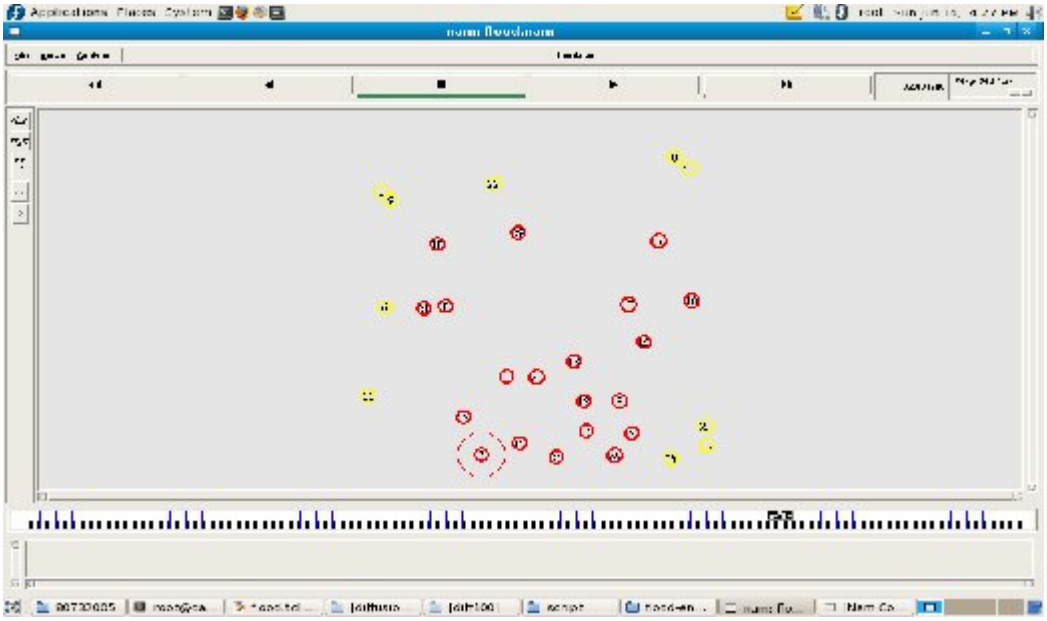


Fig. 6.3. Flooding: Network in Collapsed State

The tracegraph snapshots have been taken with the simulation time of 75 seconds. In figure 6.4, the entire simulation scenario has been displayed along with the end-to-end delay. The throughput of sending and receiving protocols has been displayed in figure 6.5 and 6.6.

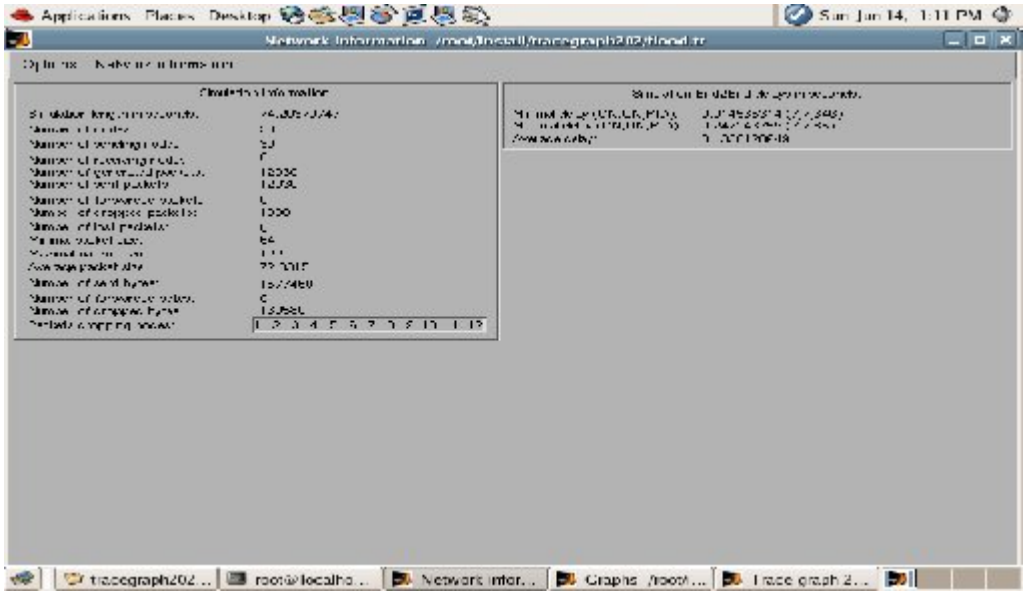


Fig. 6.4. Flooding: Simulation Details

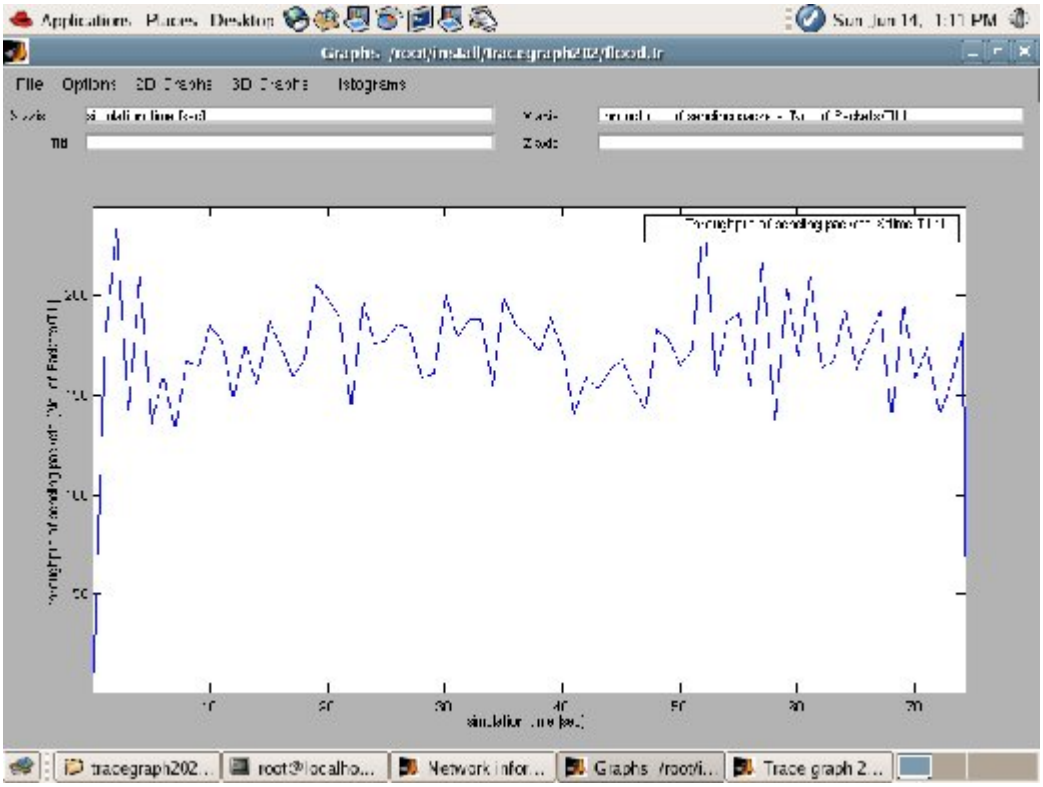


Fig. 6.5. Flooding: Throughput of Sending Packets vs Simulation Time

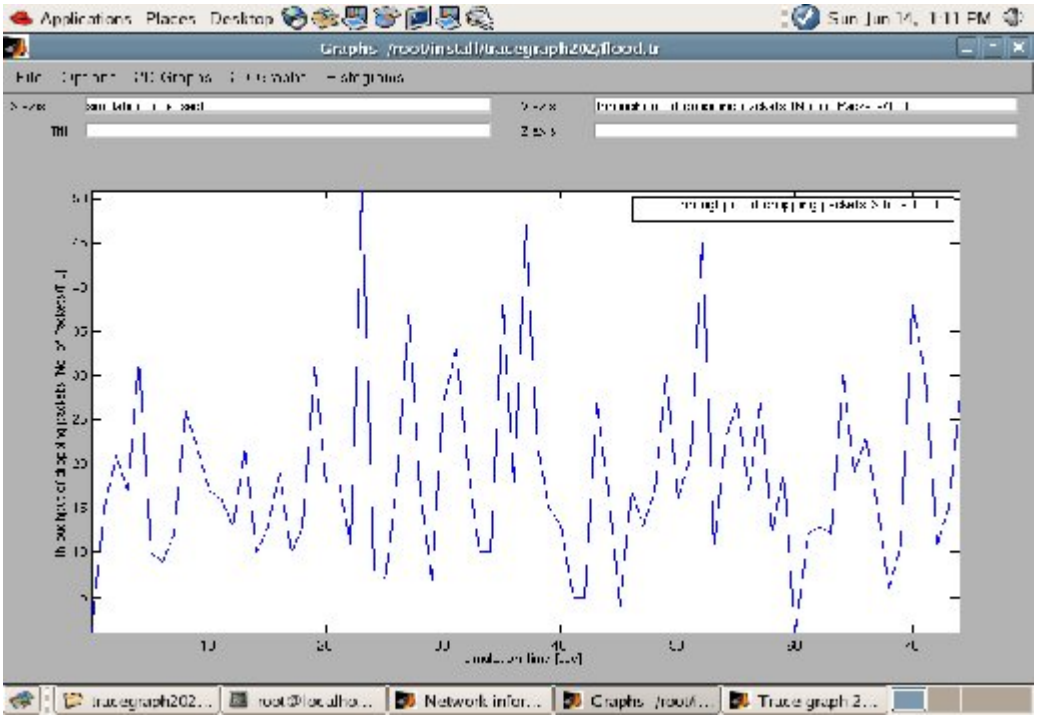


Fig. 6.6. Flooding: Throughput of Receiving Packets vs Simulation Time

End to end delay is increasing continuously because all the nodes on the straight path have lost all the energy. So to reach to the destination a comparitively long path is being followed by the message which implies the more end to end delay. In figure 6.7 end-to-end delay with its frequency distribution is being shown. The minimum delay in this scenario is 0.014s and maximum delay is 0.247s. The average delay of this flooding protocol is 0.13s. The cumulative frequency distribution has been shown in figure 6.8, which implies that the cumulative delay is increasing continually to 0.24s.

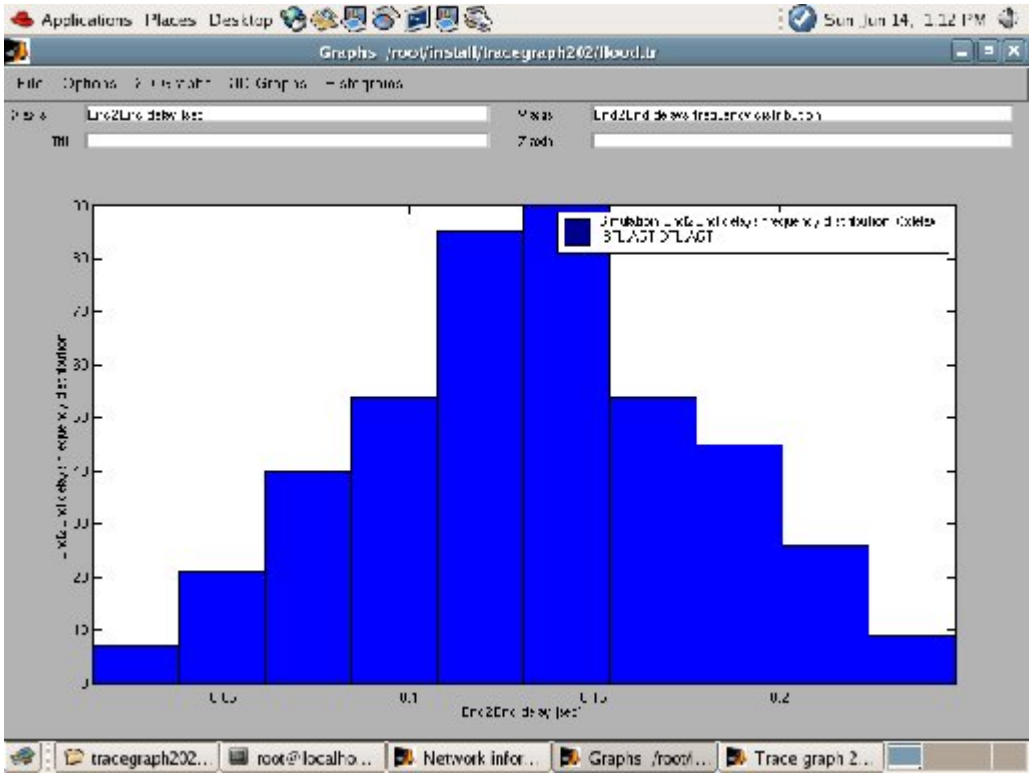


Fig. 6.7. Flooding: End-to-end Delay Frequency Distribution

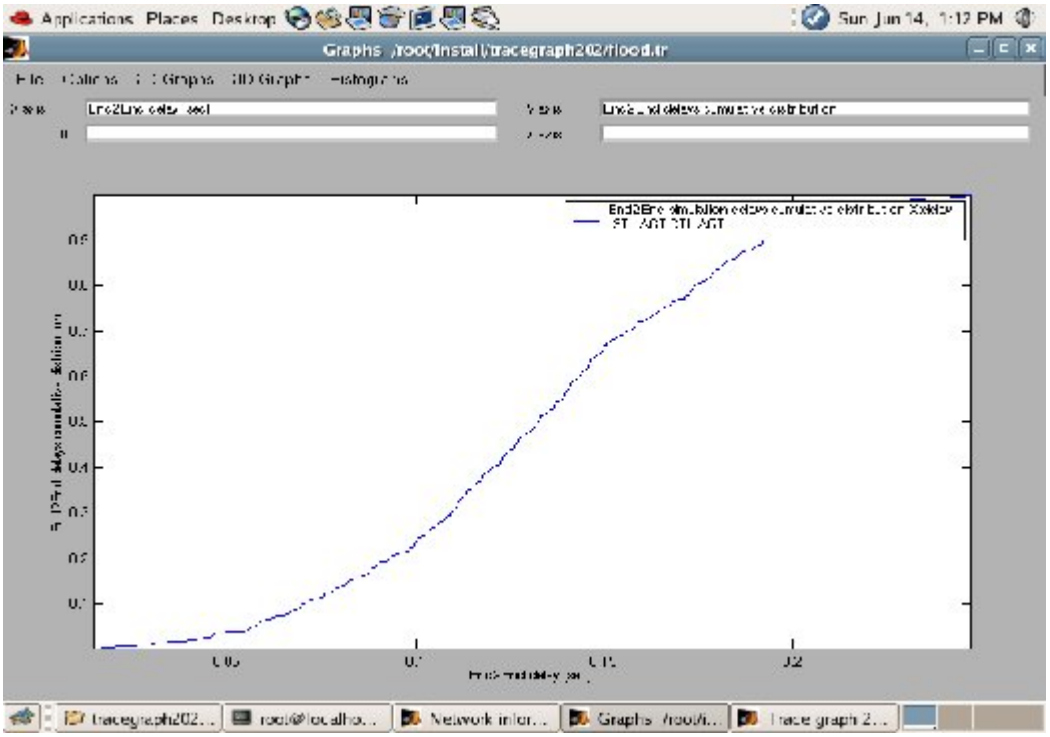


Fig. 6.8. Flooding: End-to-end Delay Cumulative Distribution

6.2. Simulation of Directed Diffusion Protocol

The same topology has been implemented for directed diffusion with same source node and same sink node. The difference between the simulation of flooding and directed diffusion is that in directed diffusion, the communication starts from sink itself. When the sink sends the interest about what it needs, source node sends a gradient in reply and then data is being delivered to the sink.

In this simulation scenario, node 7 is the source node and node 5 is the sink node. Sink node 5 sends the interest Source node 7 is sending. In figure 6.9, sink node 5 is sending interest to all the neighbouring nodes. All the nodes in the network have a cache to store the different interests. In figure 6.10, source node 7 is sending gradient back to the sink node through the same way. After a simulation time of 91 seconds, the network reaches to the crashing stage and communication between the nodes vanish completely. In figure 6.11, most of the nodes in the network have lost energy.

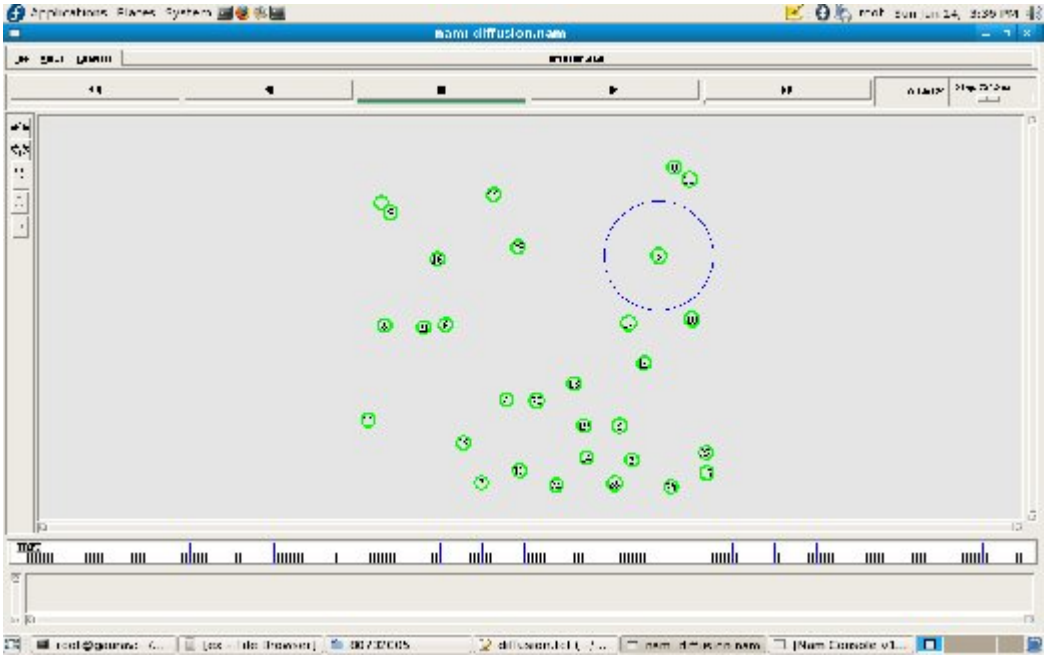


Fig. 6.9. Directed Diffusion: Sink node 5 is sending the Interest

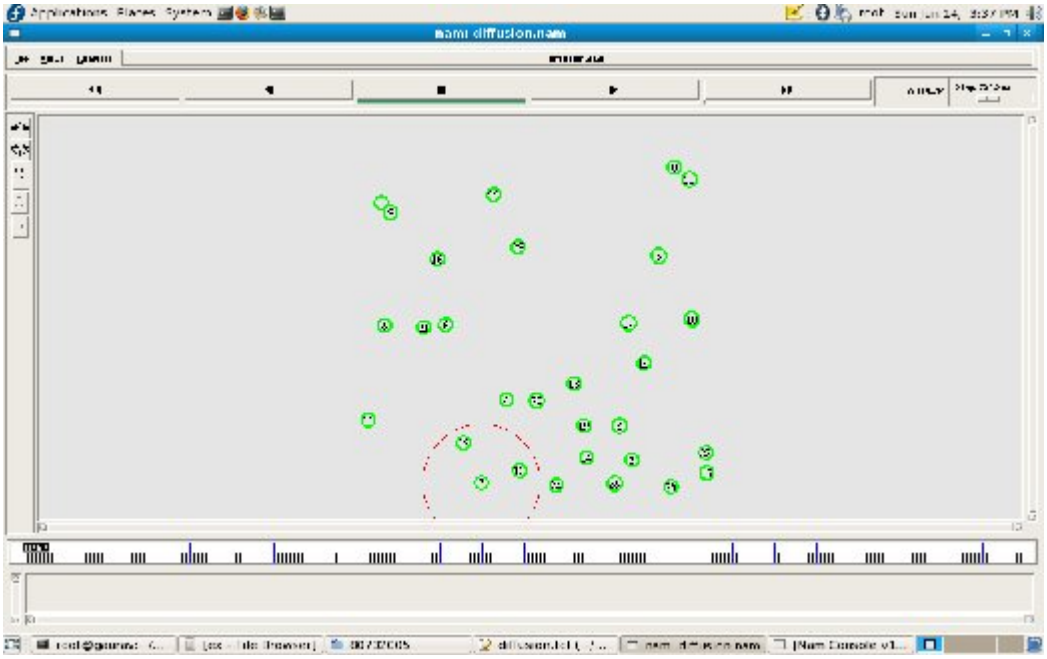


Fig. 6.10. Directed Diffusion: Source Node 7 is sending the Gradient

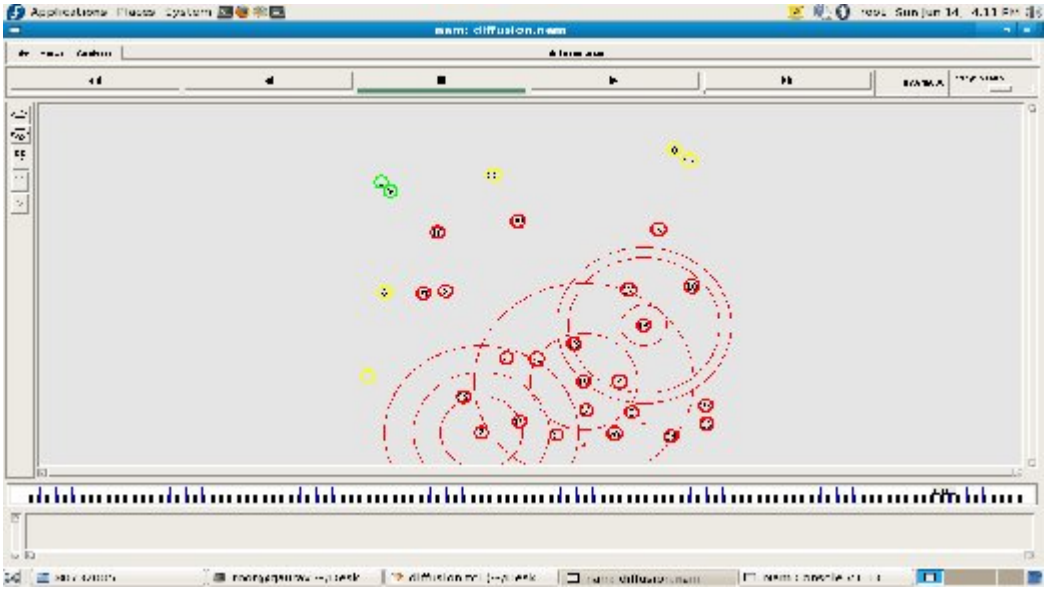


Fig. 6.11. Directed Diffusion: Network in Collapsed State

The trace file of the directed diffusion is diffusion.tr. In figure 6.12, simulation information of the sensor network has been shown. The throughput of sending, receiving packets has been shown in figure 6.13, 6.14 respectively. The number of dropped packets at all nodes has been shown in figure 6.15.

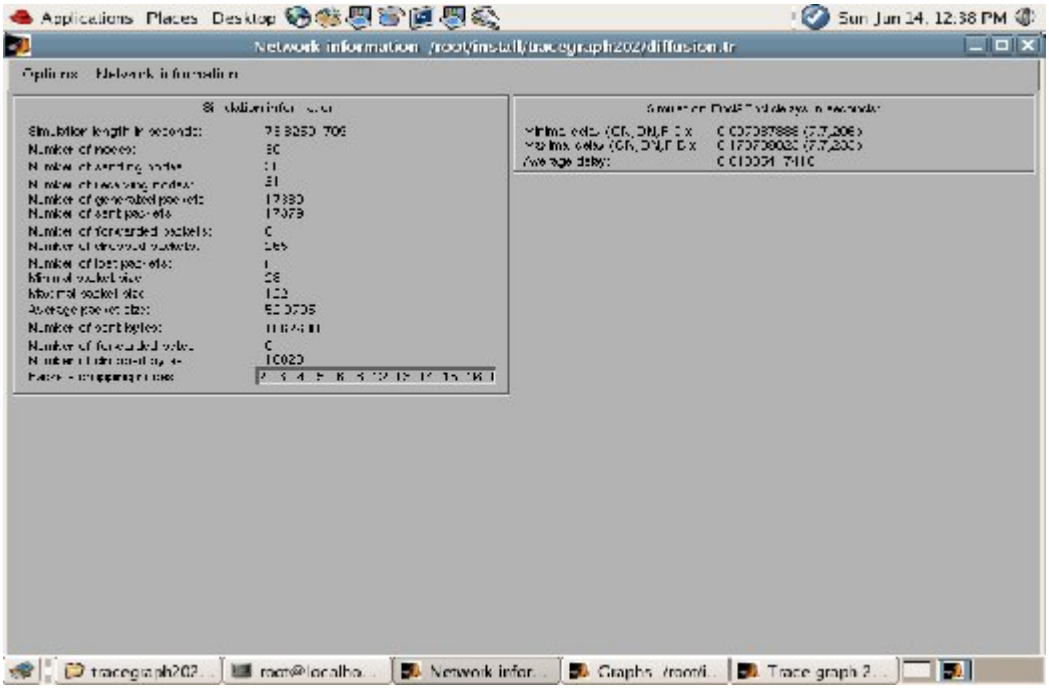


Fig. 6.12. Directed Diffusion: Simulation Details

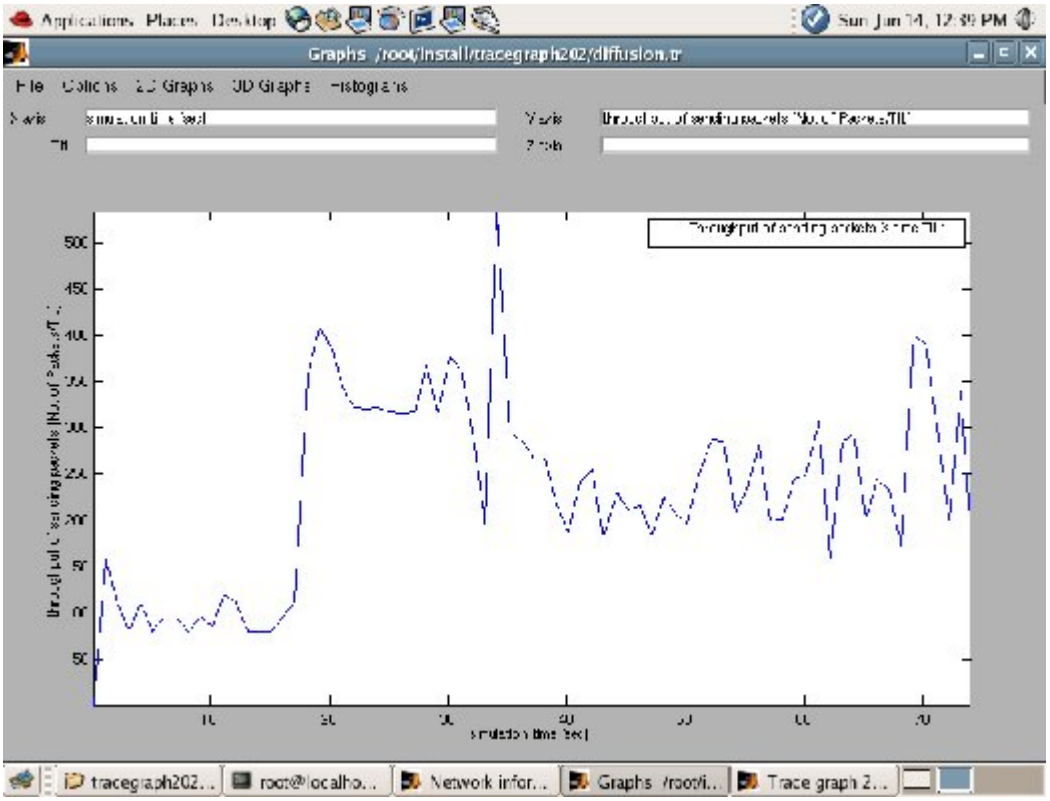


Fig. 6.13. Directed Diffusion: Throughput of Sending Packets vs Simulation Time

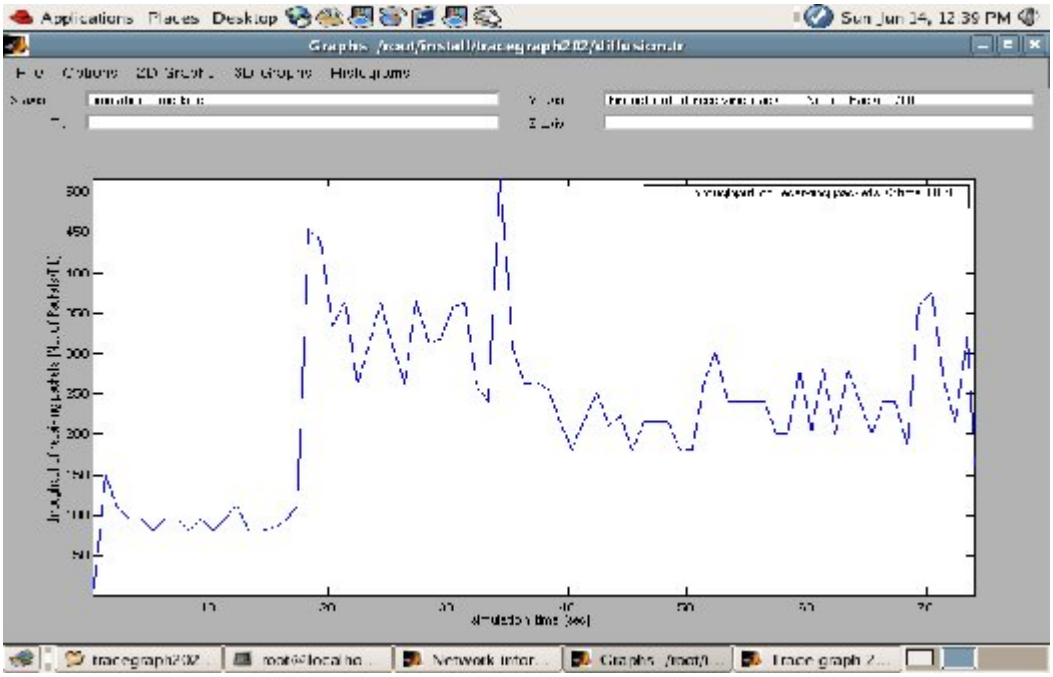


Fig. 6.14. Directed Diffusion: Throughput of Receiving Packets vs Simulation Time

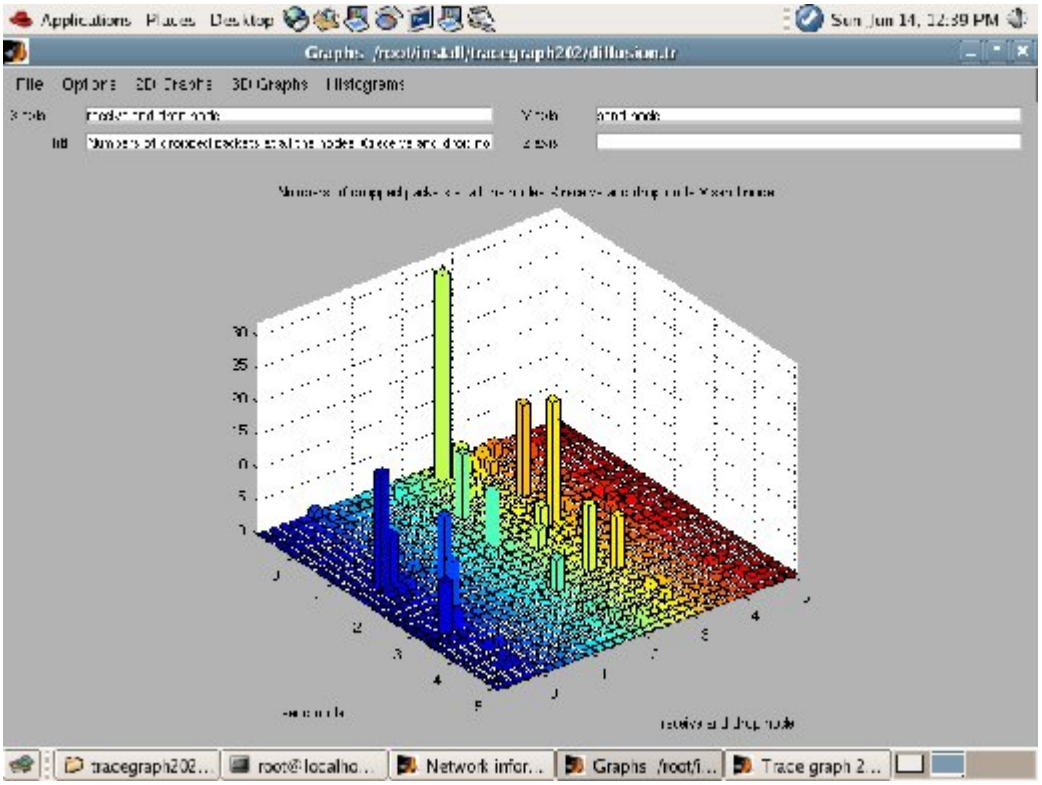


Fig. 6.15. Directed Diffusion: Dropped Packets

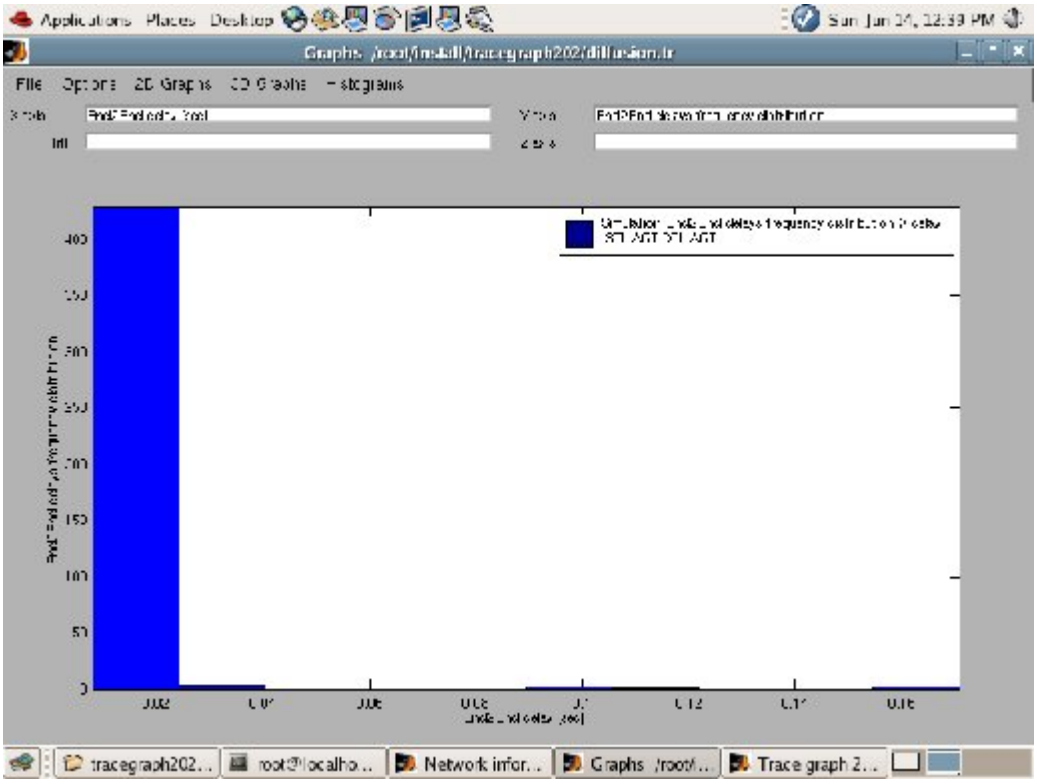


Fig. 6.16. Directed Diffusion: End-to-end Delay Frequency Distribution

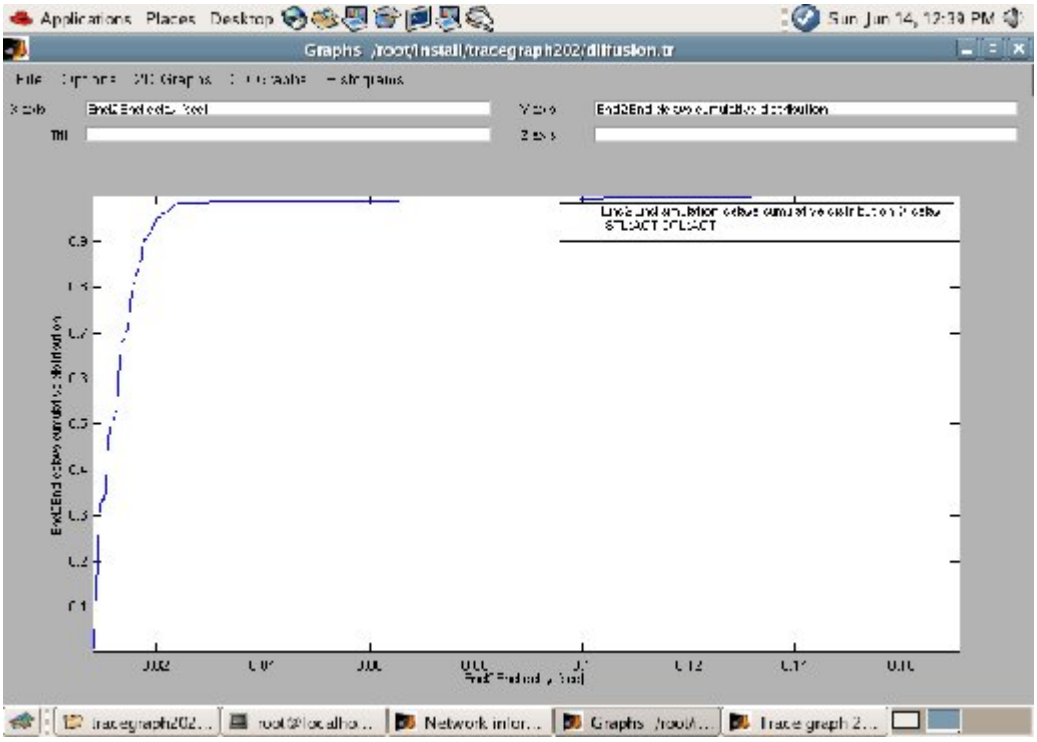
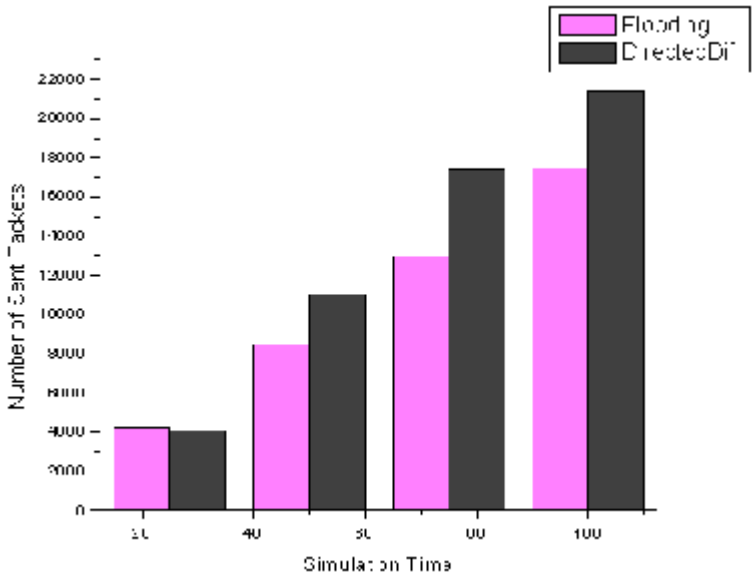
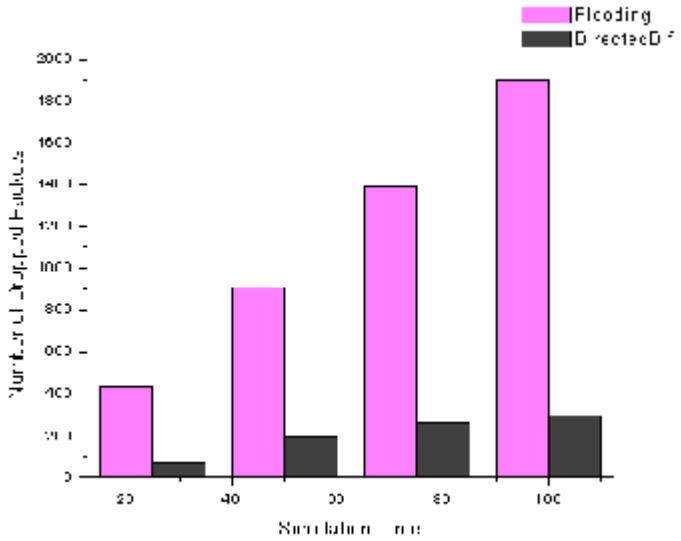


Fig. 6.17. Directed Diffusion: End-to-end Delay Cumulative Distribution

6.3. Comparison in Flooding and Directed diffusion



(a)



(b)

Fig. 6.18. Comparison in Flooding and Directed Diffusion

Table 6.1. Comparison in Flooding and Directed Diffusion Protocols

Protocol	Initial Energy (joules)	Remaining Energy (joules)	Network Lifetime (seconds)
Flooding	7	2.701	85
Directed Diffusion	7	2.904	90

6.4. Simulation of AODV Protocol

In the simulation of simple AODV, experiment is carried over 25 nodes. Through nam file it can be easily analyzed that the packets are dropping or reaching to the destination properly or not.

6.4.1. AODV Random Topology

The animation capture in figure 6.19, shows that the source is broadcasting its data to all its neighboring nodes. The source (node 20) is broadcasting RREQ message to all its neighbors and Node 4, which is the destination node, is sending RREP (route reply) back to the source. RREP in red color has been shown in figure 6.20. In figure 6.21, a packet in blue color is transmitting from the source (node 20) to the destination (node 4). As the energy of the nodes decreases, packet dropping starts. In figure 6.22, node no. 1 has lost its energy completely and a packet dropping has been shown. As the packet dropping starts, again broadcast will happen and different route will be followed.

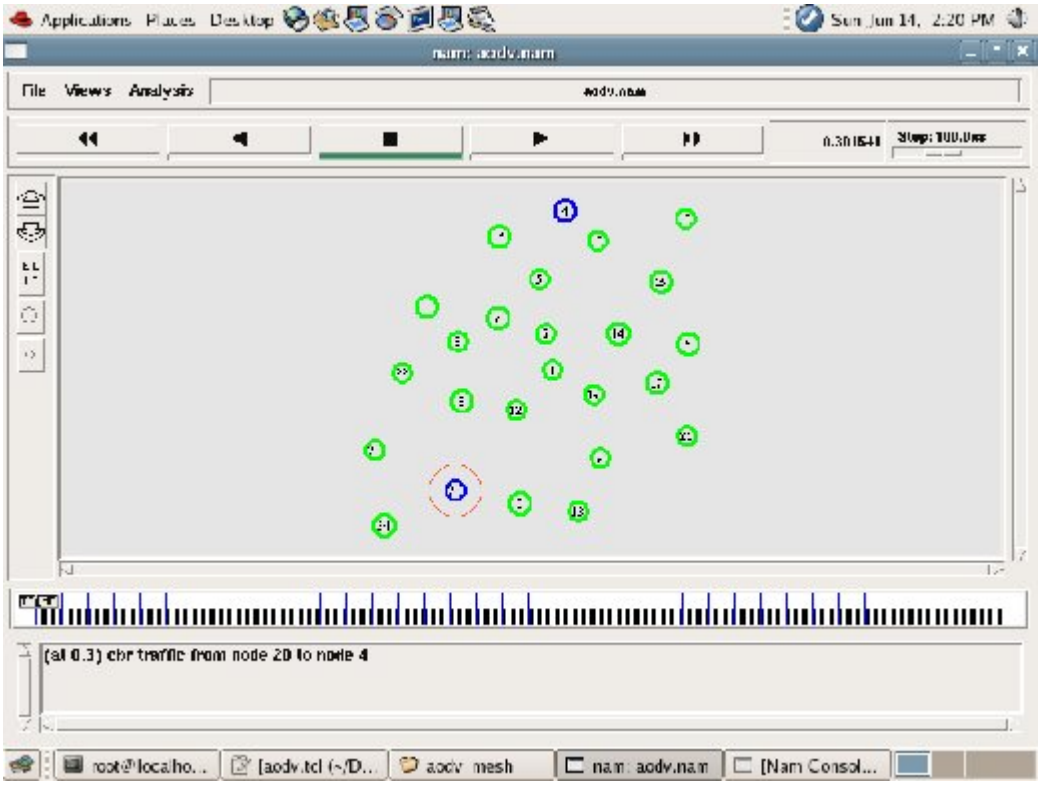


Fig. 6.19. AODV (Random Topology): Source Node broadcasts RREQ

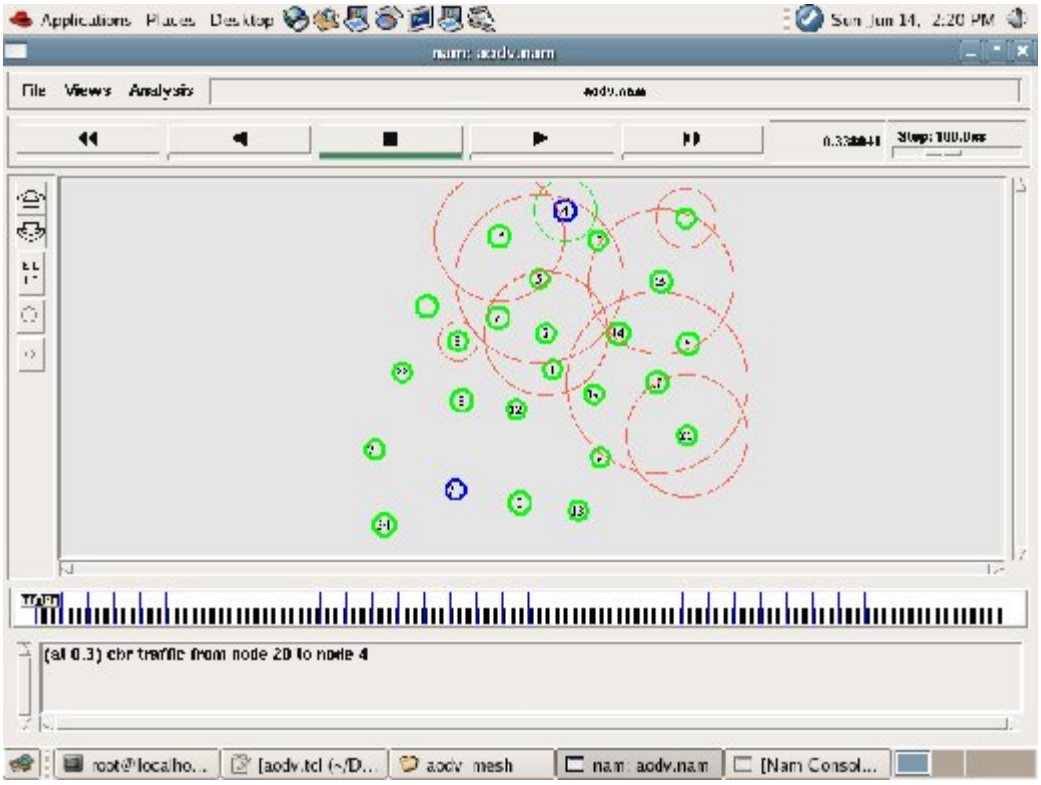


Fig. 6.20. AODV (Random Topology): Destination Node sends back RREP

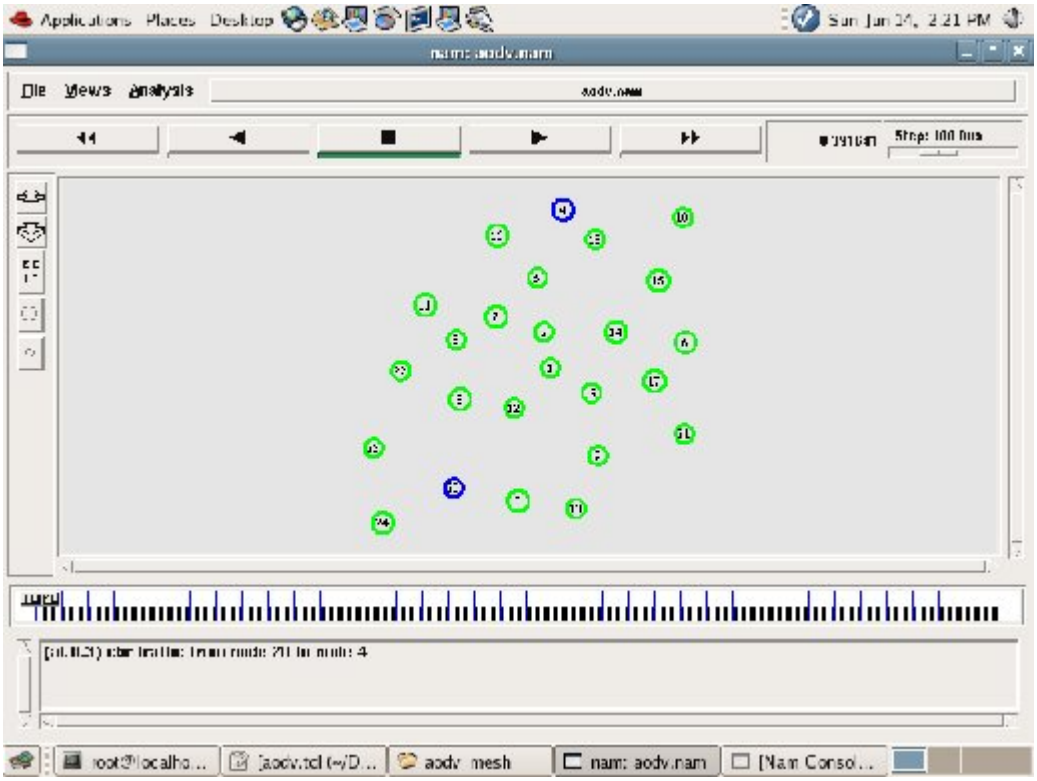


Fig. 6.21. AODV (Random Topology): Transmission of Data packets

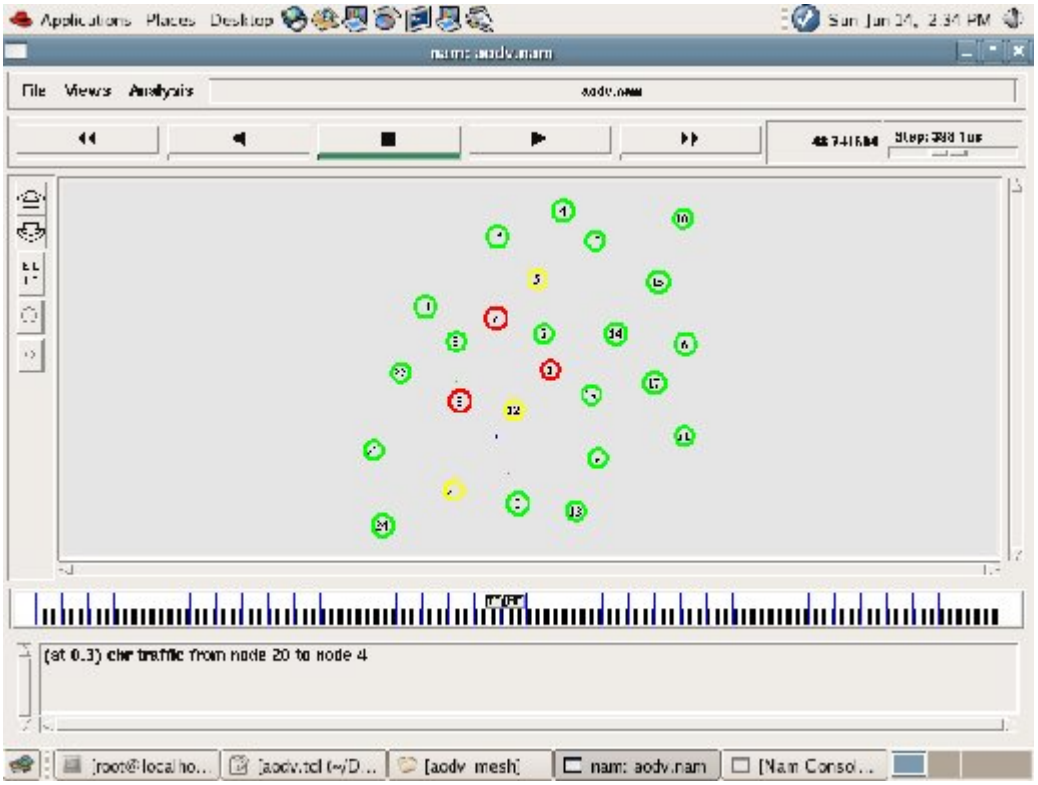


Fig. 6.22. AODV (Random Topology): Packet Drop

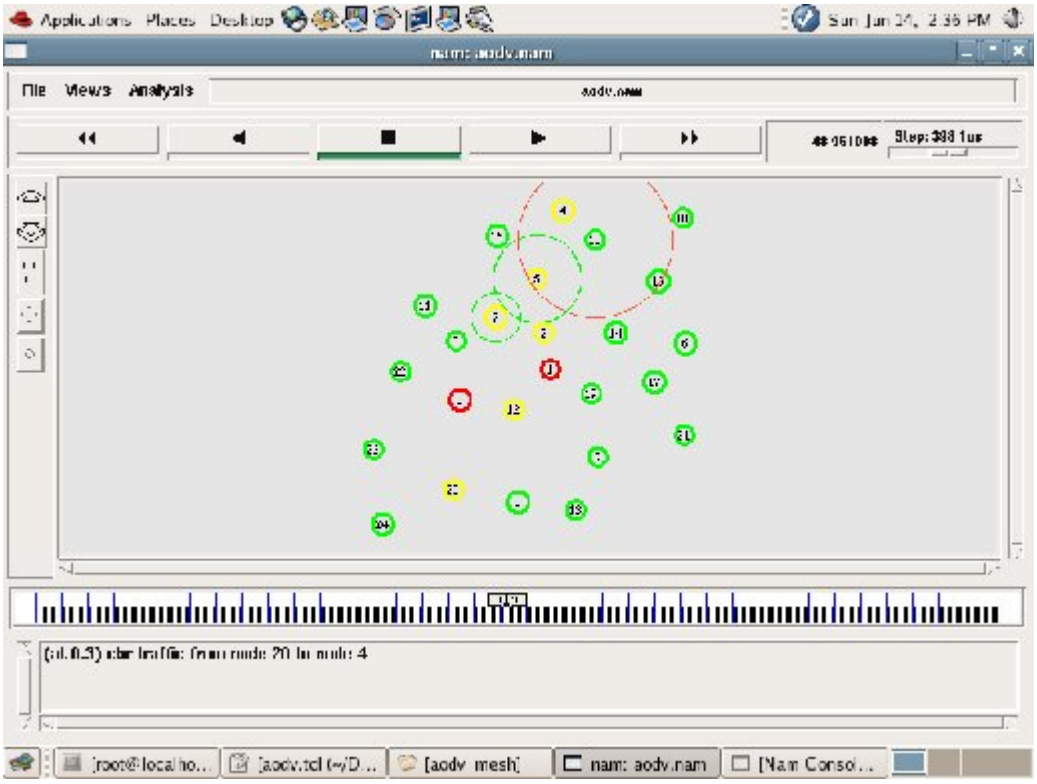


Fig. 6.23. AODV (Random Topology): Retransmission of RREQ and RREP

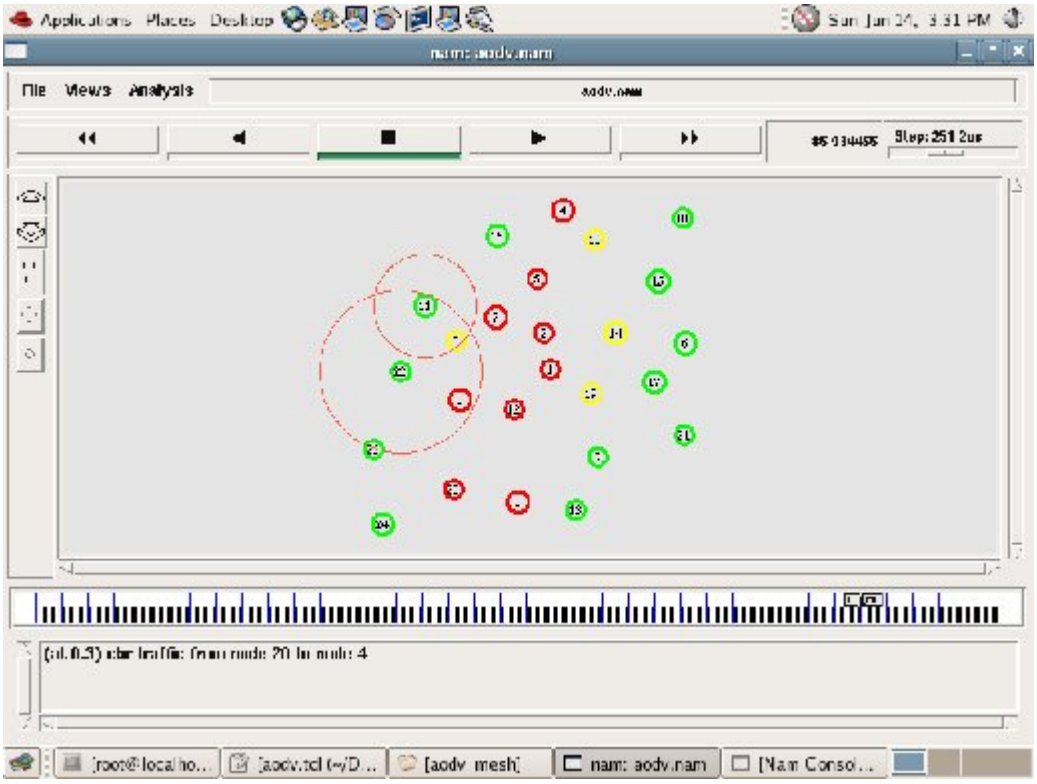


Fig. 6.24. AODV (Random Topology): Network in Collapsed State

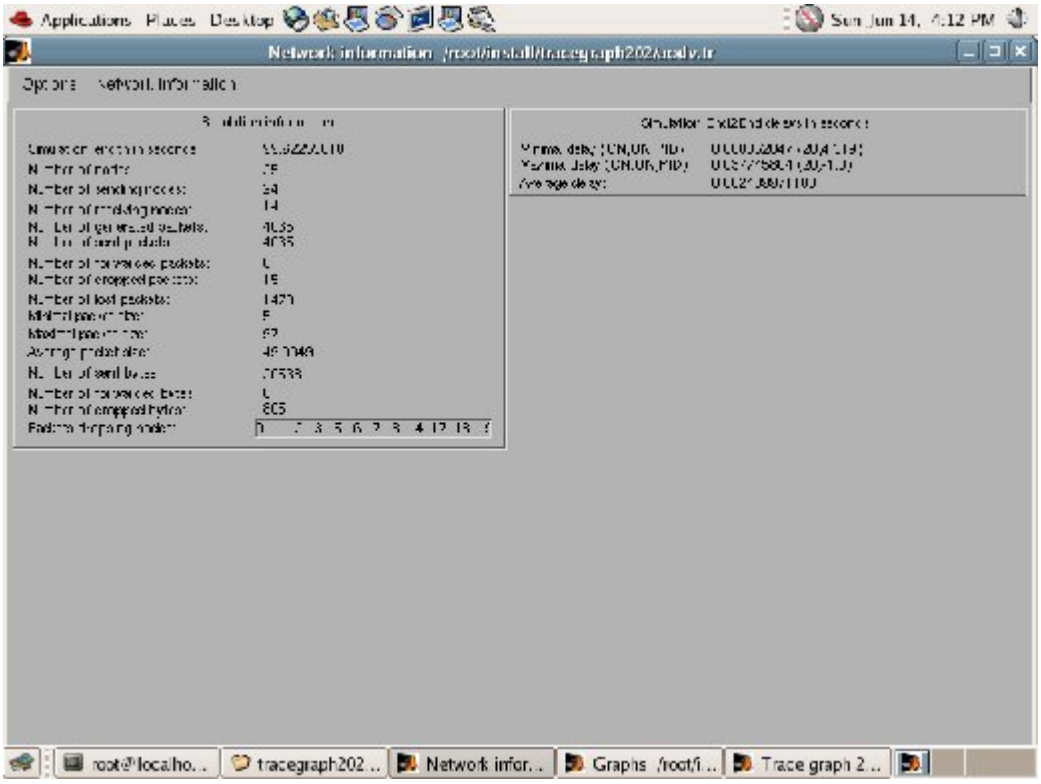


Fig. 6.25. AODV (Random Topology): Simulation Details

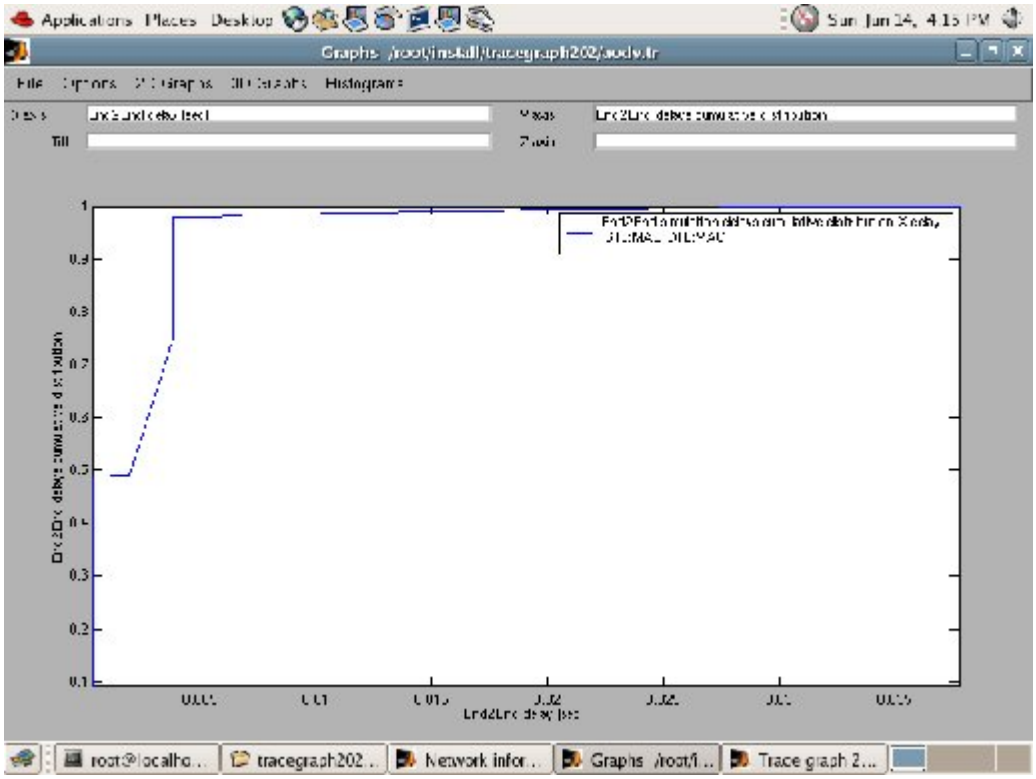


Fig. 6.26. AODV (Random Topology): End-to-end Simulation Delay Cumulative Distribution

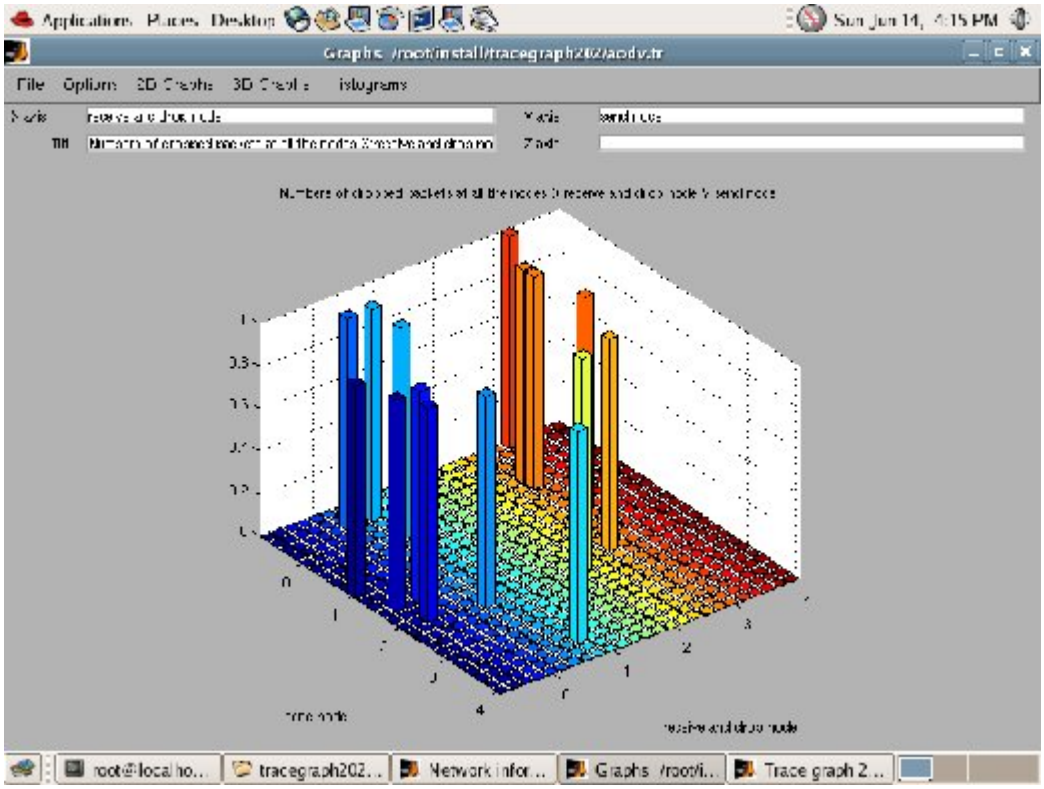


Fig. 6.27. AODV (Random Topology): Dropped Packets

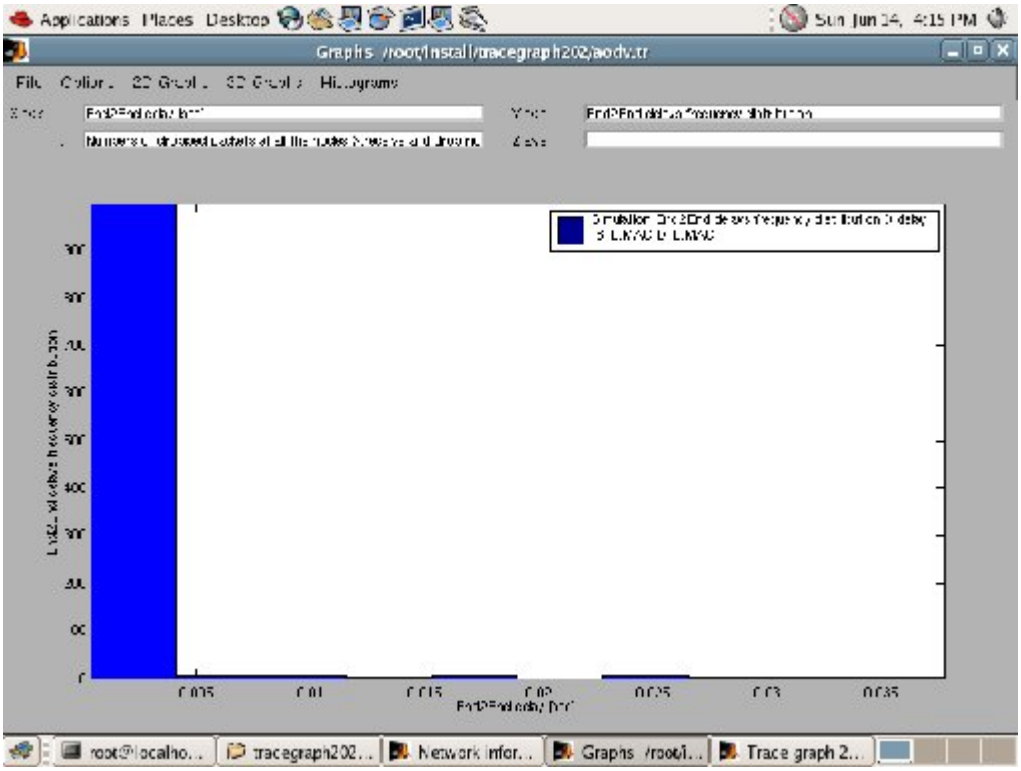


Fig. 6.28. AODV (Random Topology): Simulation End-to-end Delay Frequency Distribution

6.4.2. AODV Mesh Topology

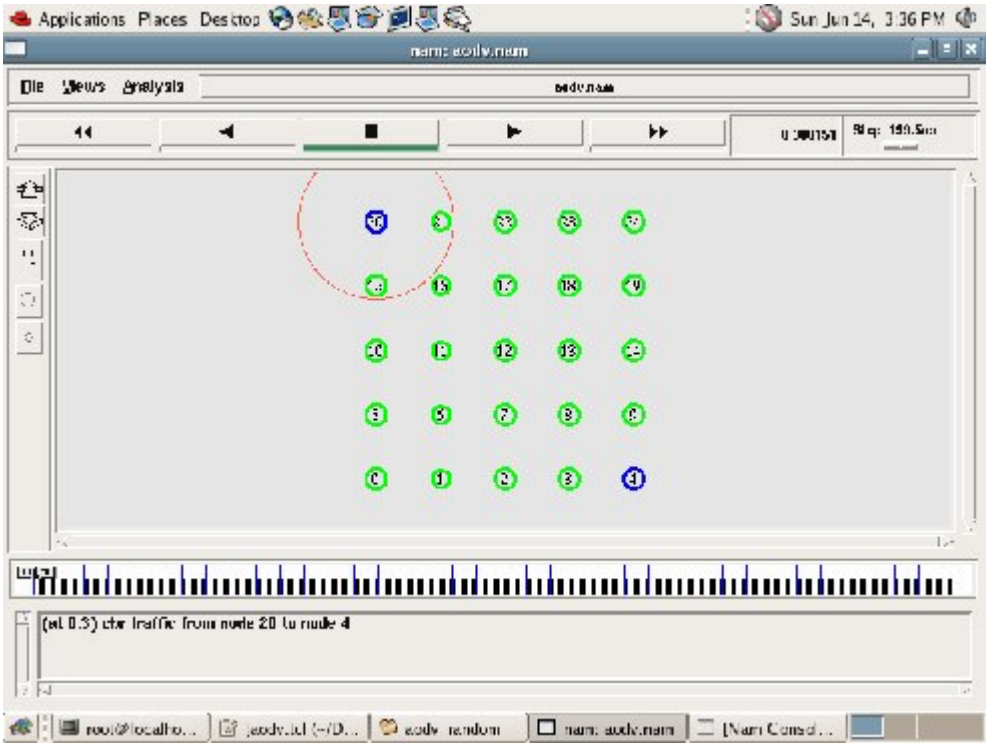


Fig. 6.29. AODV (Mesh Topology): Source Node Broadcasts RREQ

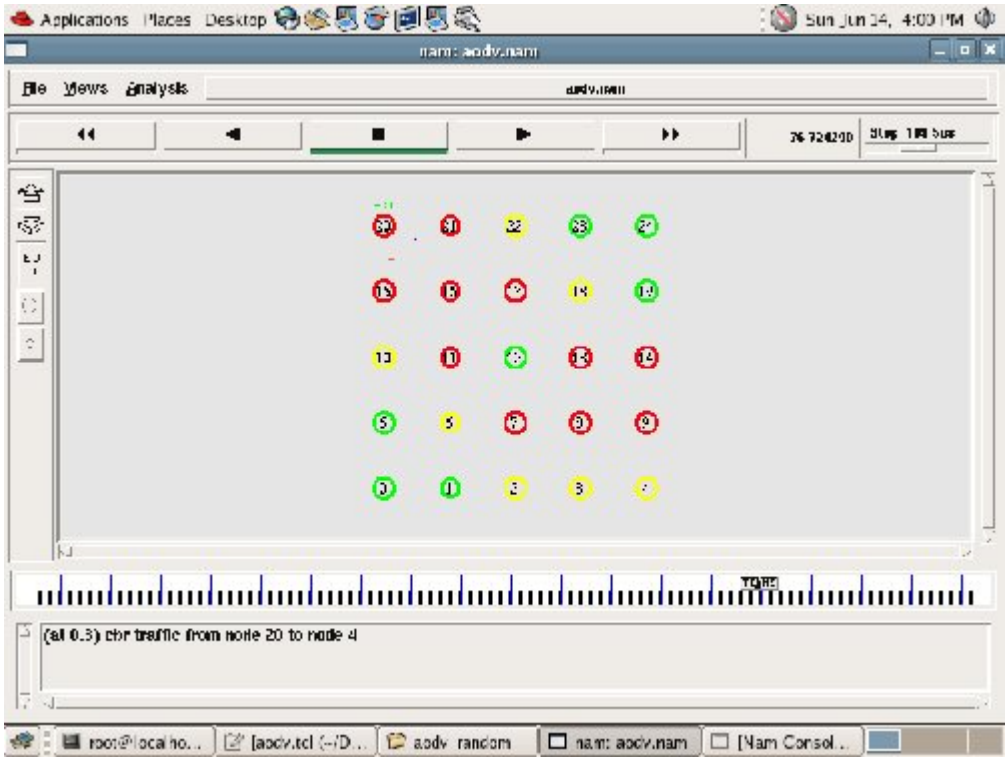


Fig. 6.30. AODV (Mesh Topology): Network in Collapsed State

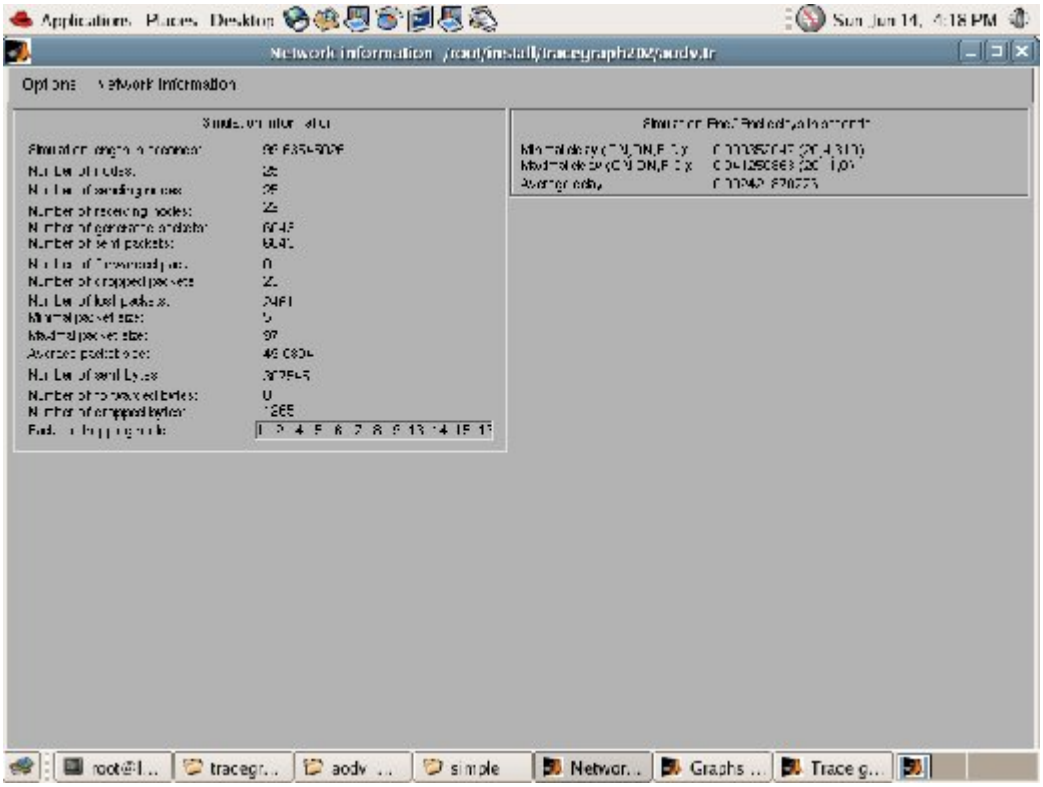


Fig. 6.31. AODV (Mesh Topology): Simulation Details

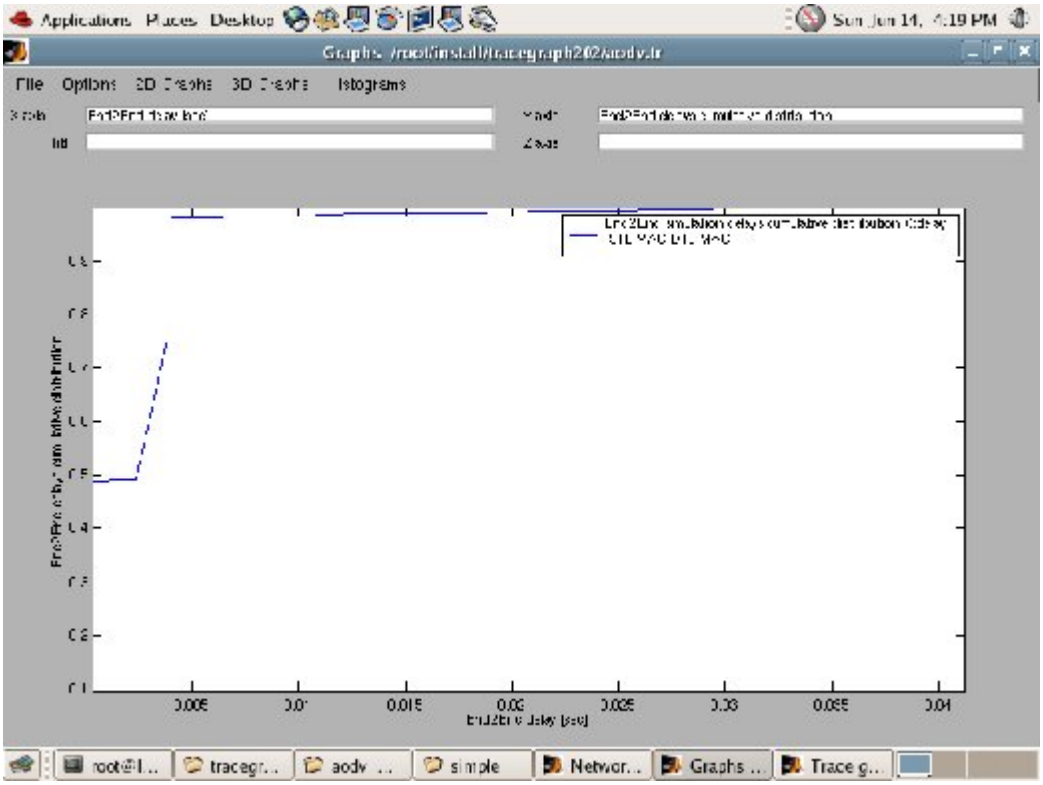


Fig. 6.32. AODV (Mesh Topology): End-to-end Simulation Delays Cumulative Distribution

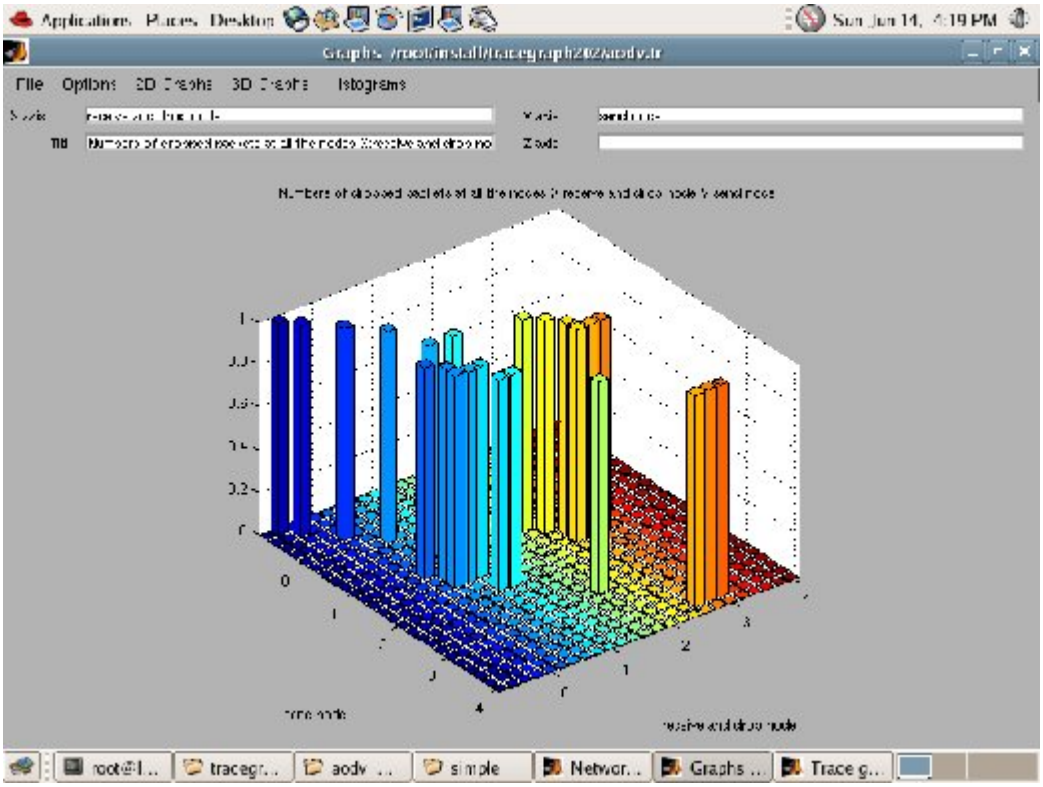


Fig. 6.33. AODV (Mesh Topology): Dropped Packets

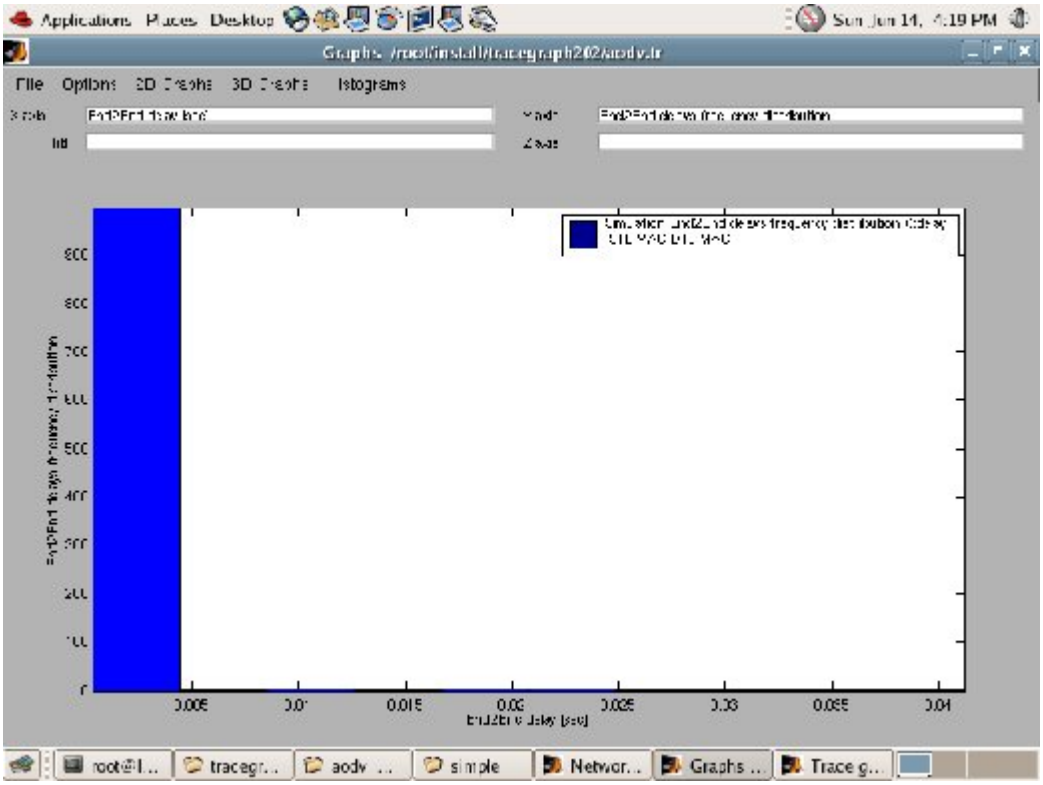


Fig. 6.34. AODV (Mesh Topology): Simulation End-to-end Delay Frequency Distribution

CHAPTER 7

CONCLUSION & FUTURE SCOPE

Routing is a significant issue in Wireless Sensor Networks. The objectives listed in the problem statement have been carried out properly. In the presented work, we have discussed a comparison of two routing protocols for wireless sensor network with different simulation times. Also AODV over WSN is simulated with different topology changes. We sincerely hope that our work will contribute in providing further research directions in the area of routing.

With the results of tracegraph, we can conclude that in the case of flooding, throughput of delivered packets is quite less than the throughput in the case of directed diffusion. Also end-to-end delay is also better in the case of directed diffusion. Since energy of the nodes is a constraint in wireless sensor network, so a fix amount of energy is given to the network in both the cases. As the simulation time increases, nodes in the network continuously lose its energy and after a fix simulation time network collapse. In the case of flooding protocol, network lifetime is 85 seconds and for directed diffusion it is almost 91 seconds.

Since Directed Diffusion is data centric so there is no need for a node addressing mechanism. Directed diffusion can reduce the bandwidth needed for sensor networks. Each node is assumed to do aggregation, caching and sensing. Directed diffusion is energy efficient since it is on demand and no need to maintain global network topology.

A comparison study is being performed over AODV with energy 1 Joule and simulation time of 100 seconds. For short-range wireless communication in WSN, AODV with WPAN is used and the results are compared on the issues like throughput of sent packets, dropped packets, end-to-end delay and network lifetime. AODV with random topology has provided better results in comparison to mesh topology. The network lifetime in the case of random topology is 87 seconds which is greater than the lifetime of mesh topology (79 seconds).

It can be concluded that the directed diffusion performs better than flooding and for short-range communication; AODV with WPAN is a nice option.

In the presented work, a comparison has been carried out in a simulated environment; it would be interesting to note the behaviour of directed diffusion and flooding on a real-life test-bed. Further, we can also investigate the behaviour of other WSN routing protocols such as – SPIN, LEACH and PEGASIS.

[1] Stephan Olariu, "*Information assurance in wireless sensor networks*", Sensor network research group, Old Dominion University.

[2] C. Chong and S. P. Kumar, "*Sensor Networks: Evolution, Opportunities, and Challenges*", in Proceedings of the IEEE, vol. 91, no. 8, Aug. 2003.

[3] Karp and H. T. Kung, "*GPSR: greedy perimeter stateless routing for wireless networks*", in *Mobile Computing and Networking*, 2000, pp. 243–254.

[4] Holger Karl and Andreas Willig. "Protocols and architectures for Wireless Sensor Networks", Wiley, 2005, ISBN:0470095105.

[5] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "*A survey on sensor networks*", IEEE Communication Magazine, Aug. 2002.

[6] Wei Yen, Ching-Wei Chen and Cheng-hsiang Yang, "*Single Gossiping with Directional Flooding Routing Protocol in Wireless Sensor Networks*", in Proceedings IEEE, 2008.

[7] K. Sohrabi et al., "*Protocols for self-organization of a wireless sensor network*", IEEE Personal Communications 7 (5) (2000) 16–27.

[8] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva, "*Directed Diffusion for Wireless Sensor Networking*", in Proceedings IEEE/ACM, Vol. 11, No. 1, Fb 2003.

[9] A. Howard, M. J. Mataric, and G. S. Sukhatme. "*Mobile Sensor Network Deployment using Potential Fields: A Distributed, Scalable Solution to the Area Coverage Problem*. In *DARS 02*, Fukuoka, Japan, June 2002.

[10] Brain P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, "*IEEE 802.11 Wireless Local Area Networks*", IEEE Communication Magazine, Vol. 35, Sep 1997

[11] Chatschik Bisdikian, "*An overview of the Bluetooth Wireless technology*", IEEE Communication Magazine, vol. 39, Dec 2001.

[12] Elizabeth M. Royer, Charles E.Perkins, "*An Implementation of the AODV Routing Protocols"*.

[13] Ad hoc on-demand distance vector (aodv) routing. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt.

[14] IEEE 802.15.4 WPAN-LR Task Group Website: http://www.ieee802.org/15/pub/TG4.html

[15] Jose A' Gutirez et al. "*IEEE 802.15.4: A Developing for Low Rate Wireless Personal Area Network"*.

[16] Anis Koubaa, Mario ALVES, Bilel NEFZI, Ye-Qiong SONG, "*Improving the IEEE 802.15.4 Slotted CSMA-CA MAC for Time-Critical Events in Wireless Sensor Network"*.

[17] Anis Koubaa, Mario ALVES, Eduardo TOVAR, "*A Comprehensive Simulation Study of Slotted CSMA-CA for IEEE 802.15.4 Wireless Sensor Network"*.

[18] Jose A' Gutirez et al. "*IEEE 802.15.4: A Developing for Low Rate Wireless Personal Area Network"*.

[19] A. Manjeshwar, D.P. Agrawal, "*APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks"*, in: Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Ft. Lauderdale, FL, April 2002.

[20] B. Krishnamachari, D. Estrin, S. Wicker, "*Modeling data centric routing in wireless sensor networks"*, in: Proceedings of IEEE INFOCOM, New York, June 2002.

[21] C. Intanagonwiwat, R. Govindan, D. Estrin, "*Directed diffusion: a scalable and robust communication paradigm for sensor networks"*, in: Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_00), Boston, MA, August 2000.

[22] C. Schurgers, M.B. Srivastava, "*Energy efficient routing in wireless sensor networks*", in: The MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA, 2001.

[23] D. Braginsky, D. Estrin, "*Rumor routing algorithm for sensor networks"*, in: Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[24] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. "*Next Century Challenges: Scalable Coordination in Sensor Networks*". In *MobiCom 99*, Seattle, USA, Aug. 99.

[25] D. Ganesan et al., *"Highly resilient, energy efficient multipath routing in wireless sensor networks"*, Mobile Computing and Communications Review 5 (4), 2002.

[26] J. N. Al-Karaki and A. E. Kamal. *"Routing techniques in wireless sensor networks: a survey"*. In IEEE Wireless Communications, Volume 11, pp. 6-28, 2004.

[27] Kemal Akkaya, Mohamed Younis *"A survey on routing protocols for wireless sensor networks"*, in: Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250, USA, 1 September 2003.

[28] Ad hoc on-demand distance vector (aodv) routing. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt.

[29] C. K. L. Lee, X. H. Lin, and Y. K. Kwok, "*A Multipath Ad Hoc Routing Approach to Combat Wireless Link Insecurity*", Proc. ICC 2003, vol. 1, pp. 448–452, May 2003.

[30] A. Manjeshwar, D.P. Agrawal, "*TEEN: a protocol for enhanced efficiency in wireless sensor networks"*, in: Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[31] L. Li, J. Y Halpern, *"Minimum energy mobile wireless networks*" revisited, in: Proceedings of IEEE International Conference on Communications (ICC_01), Helsinki, Finland, June 2001.

[32] L. Subramanian, R.H. Katz, "*An architecture for building self configurable systems*", in: Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, Boston, MA, August 2000.

[33] M. Beigl, H.W. Gellersen, and A. Schmidt. MediaCups: "*Experience with Design and Use of Computer-Augmented Everyday Objects*". Computer Networks, Special Issue on Pervasive Computing, 25(4):401–409, March 2001.

[34] R. Shah, J. Rabaey, "*Energy aware routing for low energy ad hoc sensor networks*", in: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Orlando, FL, March 2002.

[35] S. Hedetniemi, A. Liestman, "*A survey of gossiping and broadcasting in communication networks*", Networks 18 (4) (1988) 319–349.

[36] S. Lindsey, C.S. Raghavendra, K. Sivalingam, "*Data gathering in sensor networks using the energy*delay metric*", in: Proceedings of the IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[37] S. Lindsey, C.S. Raghavendra, "*PEGASIS: power efficient gathering in sensor information systems*", in: Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, March 2002.

[38] T. He et al., "*SPEED: A stateless protocol for real-time communication in sensor networks"*, in proceedings of the ICDCS, Providence, RI, May 2003.

[39] V. Rodoplu, T.H. Ming, "*Minimum energy mobile wireless networks*", IEEE Journal of Selected Areas in Communications 17 (8) (1999) 1333–1344.

[40] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "*Energy-efficient communication protocol for wireless sensor networks"*, in: Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[41] W. Heinzelman, J. Kulik, H. Balakrishnan, "*Adaptive protocols for information dissemination in wireless sensor networks*", in: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_99), Seattle, WA, August 1999.

[42] Y. Xu, J. Heidemann, D. Estrin, "*Geography-informed energy conservation for ad hoc routing*, in: Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom_01), Rome, Italy, July 2001.

[43] Fedora website. http://docs.fedoraproject.org/install-guide/fc4/en/

[44] Marc Greis. *Ns Tutorial*. http://www.isi.edu/nsnam/ns/tutorial/index.html

[45] S. McCanne and S. Floyd. *Network Simulator*. http://www.isi.edu/nsnam/ns/

[46] TCL Tutorial. http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html

[47] Tracegraph http://www.tracegraph.com/download.html

List of Publications *Annexure II*

PUBLISHED

- Gaurav Sharma, Suman Bala and A.K.Verma, "*Routing Techniques in Wireless Sensor Networks: An Overview",* International Conference on Intelligent Systems and Networks (IISN-09), Feb 14-18, 2009.
- Gaurav Sharma, Suman Bala and A.K.Verma, "*Simulation and Analysis of AODV Protocol in Wireless Sensor Networks*", National Conference on Information Security and Networks, (ISAN-2009), June 19-20, 2009.

COMMUNICATED

- Gaurav Sharma, Suman Bala, V.K.Bhalla and A.K.Verma, "Comparison of Flooding and Directed Diffusion for Wireless Sensor Network", Fifth IEEE Conference on Wireless Communication and Sensor Networks, (WCSN-2009).