"ENERGY OPTIMIZATION IN WIRELESS SENSOR NETWORKS"

Dissertation Submitted to Jawaharlal Nehru University in Partial Fulfillment of the Requirement for the Award of the Degree of

Master of Technology

Submitted by

Mahendra Ram

Submitted to

Sushil Kumar

School of Computer & Systems Sciences
Jawaharlal Nehru University
New Delhi-110067
India

2012

JAWAHARLAL NEHRU UNIVERSITY
SCHOOL OF COMPUTER & SYSTEMS SCIENCES
NEW DELHI-110067, INDIA

CERTIFICATE

This is to certify that the dissertation entitled **"ENERGY OPTIMIZATION IN WIRELESS SENSOR NETWORKS"** being submitted by **Mr. Mahendra Ram** to the **School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi,** in partial fulfillment of the requirements for the award of the degree of **Master of Technology in Computer Science and Technology,** is a record of bonafide work carried out by him under the supervision of **Mr. Sushil Kumar, Assistant Professor**.

This work has not been submitted in part or full to any university or institution for the award of any degree or diploma.

27/07/12

(Mr. Sushil Kumar)
Supervisor
SC&SS, JNU, New Delhi

(Prof. Karmeshu)
Dean
SC&SS, JNU, New Delhi

Professor Karmeshu
School of Computer and Systems Sciences
Jawaharlal Nehru University
नई दिल्ली / New Delhi-110067

JAWAHARLAL NEHRU UNIVERSITY
SCHOOL OF COMPUTER AND SYSTEMS SCIENCES
NEW DELHI-110067, INDIA

DECLARATION

This is to certify that the dissertation entitled **"ENERGY OPTIMIZATION IN WIRELESSSENSOR NETWORKS"** is being submitted to the **School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi,** in partial fulfillment of the requirements for the award of degree of **Master of Technology** in **Computer Science aud Technology,** is a record of bonafide work carried out by me.

The matter embodied in the dissertation has not been submitted in part or full to any university or institution for the award of any degree or diploma.

(MAHENDRA RAM)
M. Tech (2010-2012)
SC&SS, JNU,
New Delhi-110067

Dedicated to

My Family

ACKNOWLEDGEMENTS

I would like to express my sincere thanks to my supervisor, **Mr. Sushil Kumar** for his encouragement, enthusiasm and direction provided to me during the entire duration of the proposed work. Without his valuable thoughts, recommendation, and patience, I would have never been able to complete my work.

I wish to thank all my fellow students for their help and support. I gratefully acknowledge the unselfish help given to me by them who inspired me greatly through many interesting discussions, support, and feedbacks.

Also, I am thankful to my family for their dogged persistence and motivations in getting me complete my degree.

Finally, I want to thank the almighty whose choicest blessings have sailed me through this research effort.

MAHENDRA RAM

ABSTRACT

Since sensor nodes are powered by battery and in most situations, sensor nodes are deployed in a harsh or hostile environment, where it is very difficult to change or recharge the batteries of sensor nodes in wireless sensor networks. So energy efficiency is a central challenge in sensor networks and the radio is a major contributor to overall energy node consumption. Other critical parameters such as delay, adaptability to traffic conditions, scalability, system fairness, throughput and bandwidth utilization are mostly dealt as secondary objectives.

Some sensor network applications adopt IEEE 802.11-like MAC protocol, which is however, not a good solution for sensor network applications because it suffers from energy inefficiency problem.

In this dissertation we study an energy optimization MAC (EO-MAC) protocol, which is based on adaptive radio low-power sleep modes withcurrenttraffic conditions in the network. It provides an analytical model to conduct a comparative study ofdifferent MAC protocols (DMAC, and IEEE802.15.4) suitable for reduction of energy consumption inwireless environment. The main contribution of our work is to introduce RFID impulse protocol enhanced with adaptive low-power modes. This technique exposes the energy trade-offs of different MAC protocols. It first introduces a comprehensive node energy model, which includes energy components for radio switching, transmission, reception, listening, and sleeping for determining the optimal sleep mode and MAC protocol to use for a given traffic scenarios.

We simulate our proposed protocol i.e. EO-MAC using ns-2.33 simulator for two parameters energy consumption and throughput, for determining the behavior of the proposed protocol. The simulation results show that our proposed EO-MAC protocol performs better than theIEEE802.15.4 and DMAC protocol in low traffic scenario in terms of energy consumption and throughput.

CONTENTS

LIST OF FIGURES, ANDTABLES

LIST OF FIGURES-

LIST OF TABLES-

Chapter 1

WIRELESS SENSOR NETWORKS

1.1 INTRODUCTION

The advancement in the microelectronic-mechanical systems, memory, wireless networking and communication technologies have motivated the way for the deployment of wireless sensor nodes [36]. Wireless sensor nodes are small devices with low cost. Some are so small that is the form of dust, so that it would be extremely hard for enemies to detect and destroy them. A sensor node typically consists of four basic components: a sensing unit, a processing unit, a communication unit, and a power unit. A wireless sensor network (WSNs) typically consists of a large number of sensor nodes densely deployed in a region of interest, and one or more data sinks or base stations that are located close to or inside the sensing region. The sink(s) sends queries or commands to the sensor nodes in the sensing region while the sensor nodes collaborate to accomplish the sensing task and send the sensed data to the sink(s) for example, the internet.

It collects data from the sensor nodes, performs simple processing on the collected data, and then sends relevant information (or the processed data) via the Internet to the users who requested it or use the information. Most sensor networks consist of a large number of sensor nodes, from hundreds to thousands or even more. Node deployment is usually application dependent, which can be either manual or random. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. The sensor nodes must autonomously organize themselves into a communication network before they start to perform a sensing task. According to the deployment of sensor nodes, a sensor network can be:

- Deterministic or
- Nondeterministic [41]

Deterministic sensor network: In this sensor network, the positions of sensor nodes are preplanned and are fixed once deployed. This type of network can only be used in some limited situations, where the preplanned deployment is possible.

Nondeterministic sensor networks: In most situations, it is difficult to deploy sensor nodes in a preplanned manner due to harsh or hostile environments. Therefore sensor nodes are randomly deployed without preplanning.

Obviously, nondeterministic networks are more scalable and flexible, but require higher control complexity.

1.2 WIRELESS SENSOR NETWORK'S CHARACTERISTICS

Wireless sensor networks have the following unique characteristics [41]:

- **Dense Node Deployment:** Sensor nodes are densely deployed in a field of interest.
- **Battery - Powered Sensor Node:** Sensor nodes are powered by battery. In most situations, sensor nodes are deployed in a harsh or hostile environment, where it is very difficult to change or recharge the batteries.
- **Severe Energy, Computation, and Storage Constraints:** Sensor nodes are highly limited in energy, computation, and storage capacities.
- **Self – Configurable:** *Since* sensor nodes are randomly deployed. SO once deployed, sensor nodes have to autonomously configure themselves into a communication network.
- **Application Specific:** Sensor networks are application specific. A network is usually designed and deployed for a specific application. The design requirements of a network change with its application.

- **Unreliable Sensor Nodes:** Sensor nodes are usually deployed in harsh or hostile environments and operate without attendance. They are prone to physical damages or failures.
- **Frequent Topology Change:** Network topology changes frequently due to node failure, damage, addition, energy depletion, or channel fading.
- **No Global Identification*:*** Due to the large number of sensor nodes, it is impossible to build a global addressing scheme for a sensor network because it would introduce a high overhead for the identification maintenance.
- **Many - to - One Traffic Pattern:** In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many - to - one traffic pattern.
- **Data Redundancy:** In most sensor network applications, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

1.3 WIRELESS SENSOR NETWORKS VS. AD-HOC WIRELESS NETWORKS

Wireless sensor networks share similarities with ad-hoc wireless networks. The dominant communication method in both is multi-hop networking, but there is some distinction between them.

- Ad-hoc networks support routing between any pair of nodes whereas sensor networks have a more specialized communication pattern.
- Most traffic in sensor networks can be classified into one of three categories:
  1. **Many-to-one:** Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.
  2. **One-to-many:** A single node (typically a base station) multicasts or floods a query or control information to several sensor nodes.
  3. **Local communication:** Neighboring nodes send localized messages to discover and coordinate with each other.
- A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor.

- Nodes in ad-hoc networks have generally been considered to have limited resources, but sensor nodes are even more constrained. Of all of the resource constraints, limited energy is the most pressing.
- Sensor nodes are densely deployed. Sensor nodes are prone to failures. The topology of a sensor network changes frequently.
- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.

1.4 WIRELESS SENSOR NETWORKS APPLICATIONS

There are many applications[41] of wireless sensor networks. For example, in Environmental monitoring, Military, Health care, Industrial process control, Security and Surveillances, and Home intelligence. These are explained bellow-

1.4.1 ENVIRONMENTAL MONITORING

Sensors are used to monitor a variety of environmental parameters [37], [38], [39].or conditions.

- **Habitat Monitoring:** Sensors can be used to monitor the conditions of wild animals or plants in wild habitats, as well as the environmental parameters of the habitats.
- **Air or Water Quality Monitoring:** Sensors can be deployed on the ground or under water to monitor air or water quality. For example, water quality monitoring can be used in the hydrochemistry field. Air quality monitoring can be used for air pollution control.
- **Hazard Monitoring:** Sensors can be used to monitor biological or chemical hazards in locations, for example, a chemical plant or a battlefield.
- **Disaster Monitoring:** Sensors can be densely deployed in an intended region to detect natural or non - natural disasters. For example, sensors can be scattered in forests or revivers to detect forest fires or floods. Seismic sensors can be instrumented in a building to detect the direction and magnitude of a quake and provide an assessment of the building safety.

1.4.2 MILITARY APPLICATIONS

WSNs are becoming an integral part of military command, control, communication, and intelligence (C3I) systems [4]. Wireless sensors can be rapidly deployed in a battlefield or hostile region without any infrastructure. Due to ease of deployment, self - configurability, untended operation, and fault tolerance, sensor networks will play more important roles in future military C3I systems and make future wars more intelligent with less human involvement.

- **Battlefield Monitoring:** Sensors can be deployed in a battlefield to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing force.
- **Object Protection:** Sensor nodes can be deployed around sensitive objects, for example, atomic plants, strategic bridges, oil and gas pipelines, communication centers, and military headquarters, for protection purpose.
- **Intelligent Guiding:** Sensors can be mounted on unmanned robotic vehicles, tanks, fighter planes, submarines, missiles, or torpedoes to guide them around obstacles to their targets and lead them to coordinate with one another to accomplish more effective attacks or defences.
- **Remote Sensing:** Sensors can be deployed for remote sensing of nuclear, biological, and chemical weapons, detection of potential terrorist attacks, and reconnaissance [4].

1.4.3 HEALTH CARE APPLICATIONS

WSNs can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems [5].

- **Behavior Monitoring:** Sensors can be deployed in a patient's home to monitor the behaviors of the patient. For example, it can alert doctors when the patient falls and requires immediate medical attention. It can monitor what a patient is doing and provide reminders or instructions over a television or radio.

- **Medical Monitoring:** Wearable sensors can be integrated into a wireless body area network (WBAN) to monitor vital signs, environmental parameters, and geographical locations, and thus allow long - term, noninvasive, and ambulatory monitoring of patients or elderly people with instantaneous alerts to health care personal in case of emergency, immediate reports to users about their current health statuses, and real - time updates of users 'medical records [3].

1.4.4 INDUSTRIAL PROCESS CONTROL

In industry, WSNs can be used to monitor manufacturing processes or the condition of manufacturing equipment. For example, wireless sensors can be instrumented to production and assembly lines to monitor and control production processes. Chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. Tiny sensors can be embedded into the regions of a machine that are inaccessible by humans to monitor the condition of the machine and alert for any failure.

1.4.5 SECURITY AND SURVEILLANCE

WSNs can be used in many security and surveillance applications. For example, acoustic, video, and other kinds of sensors can be deployed in buildings, airports, subways, and other critical infrastructure.

1.4.6 HOME INTELLIGENCE

WSNs can be used to provide more convenient and intelligent living environments for human beings.

- **Smart Home:** Wireless sensors can be embedded into a home and connected to form an autonomous home network. For example, a smart refrigerator connected to a smart stove or microwave oven can prepare a menu based on the inventory of the refrigerator and send relevant cooking parameters to the smart stove or microwave oven, which will set the desired temperature and time for cooking [2]. The contents and schedules of TV, VCR, DVD, or CD players can be monitored and controlled remotely to meet the different requirements of family members.

- **Remote Metering:** Wireless sensors can be used to remotely read utility meters in a home, for example, water, gas, or electricity, and then send the readings to a remote center through wireless communication [1]. In addition to the above applications, self - configurable WSNs can be used in many other areas, for example, disaster relief, traffic control, warehouse management, and civil engineering. However, a number of technical issues must be solved before these exciting applications become a reality.

1.5 CHALLENGES

Sensor networks are a special category of ad hoc wireless sensor networks that are used to provide a wireless communication infrastructure among the sensors deployed in a specific application domain. Sensor networks present certain design challenges/issues due to the following reasons [2]:

- Sensor nodes usually do not require any kind human intercession because they are randomly deployed. Therefore the sensor network must have self-organizing capabilities. Hence the setup and maintenance of the sensor network should be entirely autonomous.

- Sensor nodes should be able to coordinate their actions with each other, so that the ordering of detected events can be performed without any uncertainty.

- Since sensor nodes use batteries for their operation which are difficult to recharge or replace when consumed (remember that often sensor nodes are deployed in remote and hostile environments), it is critical to design algorithms and protocols in such a way to utilize minimal energy. To do so, implementers must reduce communication between sensor nodes, simplify computations and apply lightweight security solutions.

- The network should be scalable and flexible to the enlargement of the network's size. The communication protocols must be designed in such a way that deploying more nodes in the network does not affect routing and clustering. Rather, the protocols must be adapted to the new topology and behave as expected i.e., the network must preserve its stability. Furthermore, introducing more nodes into the network means that additional communication messages will be exchanged, so that these nodes are integrated into the existing network. This must be done in a way that a minimum number of messages need to be exchanged among the sensor nodes, and thus battery is not wasted unreasonably.

- The communication over sensor networks must be made secure; because Security solutions are constrained when applying them to sensor networks. For example, cryptography requires complex processing to provide encryption to the transmitted data. Secure routing; secure discovery and verification of location, key establishment and trust setup, and attacks against sensor nodes, secure group management and secure data aggregation are some of the many issues that need to be addressed in a security context.

- Sensor networks are infrastructure-less. Thus all routing and maintenance algorithms need to be distributed.

- Many applications which are tracking an object require knowing the exact or approximate physical location of a sensor node in order to link sensed data with the object under investigation. Furthermore, many geographical routing protocols need the location of sensor nodes to forward data among the network. Location discovery protocols must be designed in such a way that minimum information needs to be exchanged among nodes to discover their location. Since sensor nodes are energy constrained, solutions like GPS are not recommended.

- If a sensor node fails due to a technical problem or consumption of its battery, the rest of the network must continue its operation without a problem. Researchers must design adaptable protocols so that new links are established in case of node failure or link congestion. Furthermore, appropriate mechanisms should be designed to update topology information immediately after the environment changes so as to minimize unnecessary power consumption.

- Sensor networks must support real-time communication through the prerequisite of guarantees on maximum delay, minimum bandwidth, and other QoS parameters.

1.6 PROBLEM DEFINITION AND PROPOSED WORK

It is very clear that for a wireless sensor network life time it is important to save energy. There are many method which we have discussed in which some are more efficient and some are less.

- We will propose the mathematical models for energy consumption at MAC layers in wireless sensor network and
- Simulate the proposed protocol using NS2 to show the energy consumption and throughput.

Chapter 2

MEDIUM ACCESS CONTROL

2.1 INTRODUCTION

Communication among wireless sensor nodes is usually achieved by means of a unique radio channel. It is the characteristic of the channel that only a single node can transmit a message at any given time, because a radio channel cannot be accessed simultaneously by two or more nodes that are in a radio intervention range — neighboring nodes may cause conflict at some nodes if transmitting at the same time on the same channel.

In wireless sensor networks, controlling access to the channel is usually known as *Medium access control (MAC)*. Therefore, the objective of the MAC [41] protocol is to regulate access to the shared wireless medium to ensure fair and efficient sharing and communication resources among the nodes, such that the network lifetime can be maximized.

MAC protocols in sensor networks must create a network infrastructure to establish communication links among the thousands of randomly scattered sensors.

2.2 FUNDAMENTALS OF MAC PROTOCOLSFOR WSNs

For maximizing the network lifetime, the proposed MAC protocol must be energy efficient. This can be achieved by reducing the potential energy wastes. Types of communication patterns present the behavior of the sensor network traffic that has to be handled by a given MAC protocol; the properties that must be possessed by a MAC protocol to suit a sensor network environment are outlined below.

2.2.1 COMMUNICATION PATTERNS

Three types of communication patterns are defined in wireless sensor networks [7], *broadcast, converge-cast, and local gossip*. *Broadcast* type of communication pattern is generally used by a base station (sink) to transmit some information to all sensor nodes of the network. Broadcasted information may include queries of sensor query-processing architectures, program updates for sensor nodes, control packets for the whole system. In some scenarios, the sensors that detect an intruder need to communicate with each other locally. This kind of communication pattern is called *local gossip*, where a sensor node sends a message to its neighboring nodes within a range. The sensors that detect the intruder, then, need to send what they perceive to the information center. That communication pattern is called *converge-cast*, where a group of sensors communicate to a specific sensor. The destination node could be a cluster-head, data fusion center, base station. In protocols that include clustering, cluster-heads communicate with their members and thus the intended receivers may not be all neighbors of the cluster-head, but just a subset of the neighbors. To serve for such scenarios, we define a fourth type of communication pattern; *multicast*, where a sensor sends a message to a specific subset of sensors.

2.2.2 PERFORMANCE REQUIREMENTS

Following is a brief discussion of the performance metrics [8]:

- **Delay:** *Delay* refers to the amount of time spent by a data packet in the MAC layer before it is being transmitted. In sensor networks, the importance of delay depends on the application, network traffic load, and the design choices of the MAC protocol. For time-critical applications, the MAC protocol is required to support delay-bound guarantees necessary for these applications. Guaranteed delay bounds are usually provided through careful message scheduling both locally within a communicating node and globally among all nodes in the network.

- **Scalability:** *Scalability* refers to the ability of a communication system to meet its performance characteristics regardless of the size of the network or the number of competing nodes. In WSNs the number of sensor nodes may be very large. Some nodes may die over time; some new nodes may join later; some nodes may move to different locations. A good MAC protocols should accommodate such changes gracefully. Scalability and adaptability to changes in size, density and topology are important attributes, because sensor networks are deployed in an ad hoc manner and often operate in uncertain environments.

- **Throughput:** *Throughput* (often measured in bits or bytes per second) refers to the amount of data successfully transferred from a sender node to a receiver node in a given amount of time. An important objective of a MAC protocol is to maximize the channel throughput while minimizing message delay. A related attribute is *good-put*, which refers to the throughput measured only by data received by the receiver without any errors.

- **Bandwidth Utilization:** It reflects how well the entire bandwidth of the channel is utilized in communication. It is also referred to as channel utilization or channel capacity. It is an important issue in cell phone systems or wireless LANs, since the bandwidth is the most valuable resource in such systems and service providers want to accommodate as many users as possible.

- **Fairness:** It reflects the ability of different users, nodes or applications to share the channel equally. It is an important attribute, since each user desires an equal opportunity to send or receive data for their own applications. However, at any particular time, one node may have dramatically more data to send than some other nodes. Thus rather than treating each node equally, success is measured by the performance of the application as a whole and per-node or per-user fairness becomes less important.

- **Energy Efficiency:** A sensor node is equipped with one or more integrated sensors, embedded processors with limited capability, and short-range radio communication ability. These sensor nodes are powered using batteries with small capacity. Unlike in standard wireless networks, wireless sensor nodes are often deployed in unattended environments, making it difficult to change their batteries. Furthermore, recharging sensor batteries by energy scavenging is complicated and volatile. These severe constraints have a direct impact on the lifetime of a sensor node. As a result, energy conservation becomes of paramount importance in WSNs to prolong the lifetime of sensor nodes.

2.2.3 SOURCES OF ENERGY WASTE

The major sources of energy waste [9] in a MAC protocol are:

- **Collision:** It occurs when two or more sensor nodes attempt to transmit simultaneously and the retransmissions of these packets due to collision are required, which increases the energy consumption.

- **Control Packet Overhead:** Sending and receiving control packets consumes energy too, and less useful data packets can be transmitted.

- **Idle Listening:** Listening to an idle channel in order to receive possible traffic.

- **Overhearing:** A node listens for a message that is sent to another node and for which it is not the destination.

- **Overemitting:** It is caused by the transmission of a message when the destination node is not ready to receive it.

In short, the above attributes reflects the characteristics of a MAC protocol. For WSNs, the primary factors are effective collision avoidance, energy efficiency, scalability and adaptability to densities and number of nodes. Other attributes are normally secondary.

Therefore to meet the requirement of wireless sensor networks deployments and monitoring, we translate them to a set of goals for the media access protocol. Our design goals for a MAC protocol for WSN applications [6] are:

- Low power operations
- Effective collisions avoidance
- Simple implementation
- Efficient channel utilization
- Scalable to large number of nodes

2.3 TAXANOMY OF MAC PROTOCOLS

Many surveys and introductory papers on several MAC protocols for wireless sensor networks are available in the literature [8, 9, 10, 11]. To understand the differences and commonalties of different WSN-specific MAC protocols, we will classify (*fig. 2.1*) them according to how nodes organize energy efficient access to the shared radio channel [10].

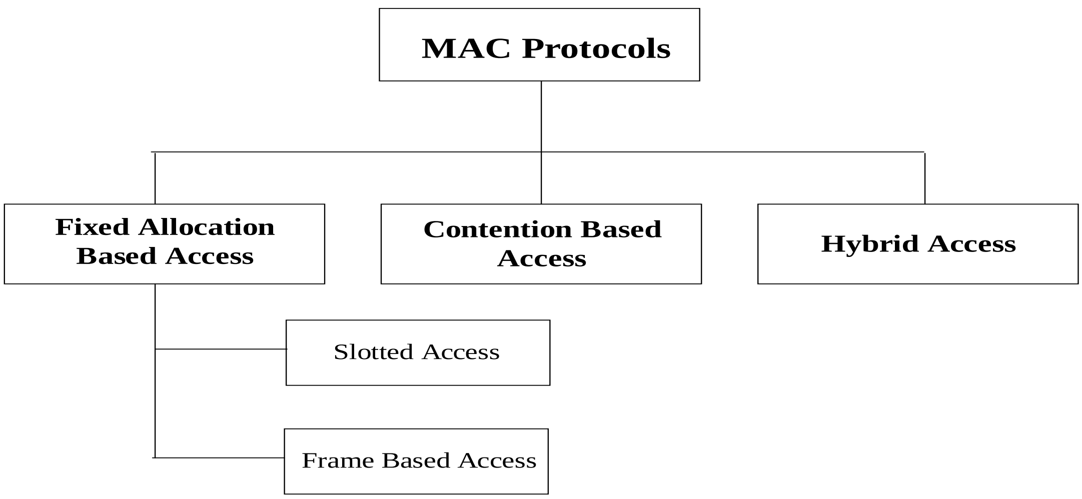

Fig. 2.1: Taxonomy of MAC Protocols

2.3.1 FIXED ALLOCATION BASED ACCESS

Fixed allocation based MAC protocols share the common channel through a predetermined fixed amount of channel resources. Each node uses its allocated resources without competing with other nodes. These protocols provide a bounded delay for each node and are suitable for sensor networks that continuously monitor and generate deterministic data traffic.

Two type of fixed allocation based access mechanism are there:

2.3.1.1 SLOTTED ACCESS

Slotted access require nodes to synchronize on some common time of references such that they can wake up collectively at the beginning of each slot and exchange messages when available; then go back to sleep for the remainder of the slot. One of the most important protocol of this category is S-MAC [12], which is a low power RTS-CTS based MAC protocol; introduces a low duty cycle operation in a multi-hop wireless sensor networks, where the nodes spend most of their time in sleep mode to reduce energy consumption.. The static sleep-listen periods of S-MAC result in high latency and lower throughput, so for overcoming these problems Timeout MAC (T-MAC) [17] was introduced which improves on the design of S-MAC by listening to the channel for only a short period of time after the synchronization phase, and if no data is received during this window, the node returns to sleep mode. If data is received, the node remains awake until no further data is received or the wake up period ends. T-MAC is aggressive in shutting down the radio, leaving messages queued for the next slot, which effectively increases latency and reduces throughput.

2.3.1.2 FRAME BASED ACCESS

In this access mechanism time is divided into frames containing a fixed number of slots. This access mechanism differs in how slots are assigned to nodes; hence collision does not occur and idle listening, overhearing can be reduced. For example, in Traffic Adaptive Medium Access (TRAMA) [29] protocol nodes are synchronized and time is divided into two cycles. In 1st cycle during, random access periods nodes exchange neighbor's information to learn about their two-hop neighbors and in 2nd cycle during, scheduled access periods nodes exchange schedules using schedule exchange protocol. Using adaptive election protocol, transmitter, receiver and stand-by nodes are elected for each transmission slot and nodes without traffic are removed from election.

Another MAC protocol called Lightweight Medium Access Control (LMAC) [19] is proposed to reduce the radio state transitions and protocol overhead. LMAC uses a distributed time slot election mechanism in which each node is able to send out a message collision-free since it owns an exclusive time slot in a two-hop neighborhood. However, all the nodes have to wake up at every time slot in order not to miss the incoming messages. The main drawback of LMAC is the fixed length of the frame, which has to be specified prior to deployment, and may be problematic. To solve this problem an Adaptive Information-centric LMAC (AI-LMAC) [20] is proposed, so that the slot assignment can be more adapted to the actual traffic needs.

2.3.2 CONTENTION BASED ACCESS

In this access mechanism also known as random access, nodes do not organize time and contend access to the radio channel; hence there is a greater possibility of collisions and lots of energy is wasted due to idle listening. Therefore random access mechanism is not suitable for real time/delay sensitive traffic. One of the most popular contention-based MAC protocol is Berkeley MAC (B-MAC) [15], which is a low complexity and low power MAC protocol whose goal is to provide a few core functionalities and an energy efficient mechanism for channel access. First, B-MAC implements basic channel access control features: a back-off scheme, an accurate channel estimation facility and optional acknowledgements. Second, to achieve a low duty cycle B-MAC uses an asynchronous sleep/wake scheme based on periodic listening called Low Power Listening (LPL), also called preamble sampling. When a sender has data to send, it transmits a preamble that is at least as long as the sleep period of the receiver. The receiver will wake up, detect the preamble, and stay awake to receive the data. This allows low power communication without the need for explicit synchronization between the nodes. The receiver only wakes for a short time to sample the medium, thereby limiting idle listening.

Another low power listening protocol i.e., X-MAC [16] is introduced, which employs a *short preamble* to further reduce energy consumption and to reduce latency. The first idea is to embed address information of the target in the preamble so that non-target receivers can quickly go back to sleep, thereby addressing the overhearing problem. The second idea is to use a *strobed preamble* to allow the target receiver to interrupt the long preamble as soon as it wakes up and determines that it is the target receiver. This short strobed preamble approach reduces the time and energy wasted during waiting for the entire preamble to complete.

2.3.3 HYBRID ACCESS

If above mentioned access mechanisms are strictly followed by any protocol; they strictly provide tighter control of who is communicating when, but at the cost of being less flexible to accommodate changing conditions. Therefore, several hybrid protocols have been developed in recent times aiming at combining the strengths of the above mentioned organizations while offsetting their weaknesses to better address the special requirements of wireless sensor network MAC protocols. The greatest advantage of the hybrid MAC protocols comes from its easy and rapid adaptability to traffic conditions, which can save a large amount of energy

For these reason recent researches in MAC area are mainly focuses on the combination of their access mechanism (e.g., CSMA/TDMA) rather than sticking only on one.

One of the most interesting hybrid protocols is Zebra MAC (Z-MAC) [21] which combines contention based access and scheduled based access mechanism by dynamically switching between the two, thus widening the scope of applications that can be supported by a WSNs. Z-MAC starts with an initial setup phase in which neighbor discovery process build a list of two-hop neighbors for each node. Then a distributed slot assignment algorithm is applied to ensure that no transmission from a node to any of its one-hop neighbor interferes with any transmission from its two-hop neighbors. Next, nodes must contend for access when wanting to send a message. By default a node may contend for any slot, but an owner gets priority by contending first. Another way of combining CSMA with TDMA is followed by Pattern MAC (PMAC) [22], which schedules (schedules are decided based on a node's own traffic and that of its neighbors) receiving slots so that a node can either be sleep or wake up in its own slot to check for incoming traffic, instead of, in every slot.

Chapter 3

RELATED WORK

A concise survey of recently proposed several MAC protocols for wireless sensor networks can be found in [8]. In this section we first give the brief idea of the IEEE 802.11, the SMAC, and the energy optimization techniques.

3.1 IEEE 802.11

IEEE 802.11 [13] is the standard MAC layer protocol which is proposed for wireless LANs. This scheme is a contention-based protocol which employs RTS/CTS control packets in order to reduce collision which may occur due to hidden and exposed node problem [6]. Beside, this, it uses both physical and virtual carrier sense mechanism to indicate the free channel. Now we define the terms *transmission range* and *carrier sensing zone* which are used for clear understanding of the proposed protocol.

- **Transmission range***:* It is the distance between sender node and its neighboring nodes that can receive and correctly decode the packets coming from the sender node. The level of power used in transmission and radio propagation properties (i.e., attenuation) determines the transmission range.

- **Carrier sensing zone***:* When a node is within the carrier sensing zone, it can sense the signal but cannot decode it correctly. It does not include transmission range because nodes in transmission range can definitely sense the transmission as well as decode it correctly.

Fig. 3.1 shows the transmission range (it may not be circular in reality) and carrier sensing zone for node M. When node M transmits a packet, node R and S can receive and decode it correctly since they are in transmission range. However, node P and Q only sense the signal and cannot decode it correctly because they are in the carrier sensing zone.

However, the IEEE 802.11 technique suffers from energy inefficiency problem. This problem is solved by S-MAC [12][14] protocol which combines the features of both Contention based as well as TDMA protocols which have been considered as the best provider for energy saving. The TDMA approach schedule transmission times of neighboring nodes to occur at different times. However, the major disadvantage of this technique is that it is not well adaptable to topology changes.

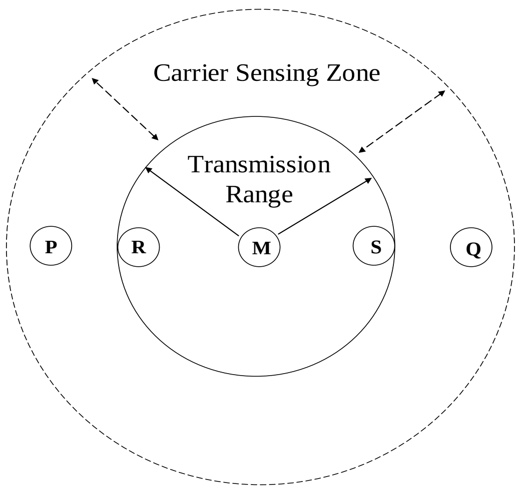

Fig. 3.1: Nodes in the transmission range can receive and decode packets correctly, whereas nodes in the carrier sensing zone can sense a transmission, but cannot decode it correctly.

3.2 S-MAC PROTOCOL

The S-MAC [12] protocol is considered to be the first standard MAC protocol which is proposed for WSNs in order to reduce energy consumption caused by from all the sources of energy waste i.e., idle listening, collision, control overhead, overhearing, and over emitting that were discussed earlier. In exchange the protocol incurs some performance reduction in per-hop fairness and latency. The S-MAC uses multiple techniques to reduce energy consumption, control overhead, and latency, in order to improve application-level performance.

1. **Periodic listen and sleep**: In S-MAC the energy lost caused by idle listening is reduced by letting nodes to go to in sleep mode periodically (as shown in below *fig. 3.2*), instead of constantly listening to an idle channel. When a node is in sleep mode its radio will be turned off, thus conserving energy.

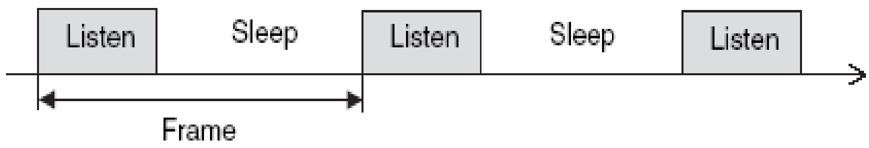

Fig. 3.2: Periodic listen and sleep

We call a complete cycle of the listen and sleep intervals, a frame. So,

$$T_{Frame} = T_{Listen} + T_{Sleep}$$

2. **Synchronizing schedules**: Synchronization between neighboring nodes is accomplished by means of broadcasting SYNC packets which are exchanged periodically between neighboring nodes. In this way, nodes make a cluster sharing the same schedule. This mechanism allows S-MAC to reduce control packets overhead. Each node in the network is free to choose its own or other nodes schedule by following below steps:

    - Listen for a sufficient amount of time to hear the existing schedule, if not, then, the node chooses its own schedule and broadcast it to its neighbors.

- If a schedule is reserved, it will be followed by the node, then broadcast after a random amount of time to avoid collisions between SYNC packets issued from nodes which select the same schedule.

- Two schedules will be followed if a new schedule is received, another is followed and broadcasted.

3. **Overhearing avoidance**: radios are turned off while the shared media is used for transmission between other nodes. However, when a node hears a RTS or a CTS packet and doesn't present the data recipient, it goes to sleep until the current transmission end.

4. **Message passing**: This scheme is used to reduce contention latency for sensor network applications requiring store-and-forward processing as data are moved through the network. In S-MAC, the RTS packet allocates the shared medium for transmitting the entire message instead of reserving the medium just for the first fragment like in IEEE 802.11. In this latter, each fragment and its ACK plays the role of RTS/CTS sequence for the next fragment.

A closer look at the periodic listen and sleep scheme reveals that a message may incur increased latency as it is stored and forwarded between adjacent network nodes. To address this shortcoming, the protocol uses a technique referred to as adaptive listening [14].The basic idea is to let the node who overhears its neighbor's transmissions (ideally only RTS or CTS) wake up for a short period of time at the end of the transmission. In this way, if the node is the next-hop node, its neighbor is able to immediately pass the data to it instead of waiting for its scheduled listen time. If the node does not receive anything during the adaptive listening, it will go back to sleep until its next scheduled listen time.

3.3 Related Works for Energy Optimization

The works related to energy optimization are -

3.3.1 ENERGY-AWARE WIRELESS COMMUNICATION:

- **LEACH:** In [23], the authors proposed the LEACH (low energy adaptive clustering hierarchy) protocol, in which a cluster head aggregates data from sensor nodes within the cluster and send the aggregated data directly to the sink. Furthermore, cluster head rotation scheme was proposed such that the role of cluster head is dynamically rotated among sensor nodes. It is shown that LEACH can improve the energy efficiency, at the cost of extra overhead due to dynamic clustering.

3.3.2 NETWORK-WIDE ENERGY OPTIMIZATION:

- **SPAN:** An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks
- **GAF:** Geography-informed energy conservation for ad hoc routing,
- **STEM:** Topology management for energy efficient sensor networks

3.3.3 CROSS-LAYER DESIGN AND OPTIMIZATION:

- Cross-layer design for lifetime maximization in interference-limited wireless sensor networks.
- Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks.

Chapter 4

PROPOSED ENERGY OPTIMIZATION MAC (EO-MAC) PROTOCOL

4.1 DESIGN OVERVIEW

Energy efficiency is a central challenge in sensor networks, as battery replacement is costly and often difficult in inaccessible deployment regions. Several efforts have addressed energy efficiency in sensor networks, through the design of energy saving MAC protocols, such as duty cycling protocols [26] or low-power wake-up radio protocols [28], and routing protocols, such as [27].

Radio energy consumption is a major component contributing to the overall energy consumption at each node. Current MAC protocols put the radio in sleep mode while there is no data to send or receive in order to minimize energy consumption. Although, most radios for sensor networks support multiple sleep modes, the radio sleep mode in current MAC protocols is static. Choosing a static low-power mode involves an energy and delay tradeoff.

Considering the adaptive radio power modes that dynamically change according to current traffic conditions in the network to address the tradeoff. To get the benefits of adaptive sleep modes, we incorporate them into RFID Impulse mechanism [29], [25], and compare its performance against the IEEE802.15.4, DMAC protocols. Basically the performance evaluation of RFID impulse protocol considers the radio energy consumption, including receiving, transmitting, listening, and sleeping energy consumption, but it disregards the switching energy component [30] that is appreciable for any protocol that switches nodes between active and sleep modes in low traffic conditions. In order to determine how to adapt low-power modes in RFID Impulse and to compare the MAC protocols, this presents a sensor node energy consumption model that includes switching energy. The model enhances existing models [26], is generalizable to any MAC protocol, and serves as the basis for revaluating the energy consumption of sleep mode configurations for given traffic loads and for determining the optimal protocol/sleep mode configuration and for comparing the protocols. The comparison of the protocols under different traffic loads yields guidelines for selecting appropriate MAC protocols for specific traffic requirements of an application. We also determine the optimal radio low power mode within RFID Impulse as the data rate varies.

4.2 MAC PROTOCOLS:

Here we have to study the three protocols that is IEEE 802.15.4, DMAC and RFID Impulse. Tacking combination of these protocols and find out which protocol is better to optimize the energy using low power sleep mode for a given scenario of wireless sensor networks.

4.2.1 IEEE 802.15.4:

IEEE 802.15.4 standard [24] defines the physical and MAC layers specifications for low data rate and energy efficient wireless networks. Since MAC layer include both a beacon enabled mode and a non-beacon-enabled mode. Here focus only on the non-beacon enabled mode because the beacon- enabled mode represents an over kill and does not perform well in long-term monitoring application. Since no beacons are broadcast in the non-beacon enabled mode so 802.15.4 reduces to plain CSMA/CA.

Nodes are used a binary exponential (BE) back off mechanism to evaluate collisions, with the variable BE defining the number of slots during each back off period. Initially the binary exponent of the back off is set to 3, so that any node selects a random time slot R1 during the first $2^{BE} - 1 = 7$ time slots to send data. During the time slot R_1a node then performs a clear channel assessment (CCA). If there is no activity on the channel, then the node assumes that the channel is free of carriers, so it reserves the channel for the time slotR_1. But if the channel is busy then the node back off and increase BE by 1 that is BE=3+1 and selects a random time slot R_2 during the next $2^4 - 1 = 15$ time slots. The CCA process is repeated. If R_2 is also busy, then the node repeats the process for BE = 5 to selectR_3 . If R_3 is free, then the node sends its data during the time slotR_3 . Otherwise, it drops the packet.

4.2.2 DMAC

The Data–Gathering Medium Access Control (DMAC) is an energy efficient and low latency MAC protocol by Lu et al [31] for data gathering in wireless sensor networks. The primary goal of DMAC is to achieve both energy efficiency and low latency. It has been designed and optimized for tree based data gathering (converge cast communication) in wireless sensor network. In this protocol the time is divided in small slots and runs carrier sensing multiple access (CSMA) with acknowledgement within each slot to transmit/receive one packet. The sensor node periodically executes the basic sequence of '1'transmit, '1' receive and 'n' sleep slots. In the sleeping period, a node turns off its radio to save energy.

4.2.3 RFID IMPULSE

Basically RFID impulse [40] is a very low-power radio wake-up scheme for sensor networks that relies on-off the shelf RFID readers and tags. The Basic functions of RFID impulse is that all network nodes turn off their radios, including the voltage regulator and the oscillator, as long as they have no packets to send or receive and sends a short acknowledgment message by the standard radio to the sender. This indicates that the RFID wake-up was successful. The sender after receiving the short acknowledgment from the receiver begins the transmission. Once the sender completes all its packet transmissions, both sender and receiver again turn off their radios. If a sender fails to receive an acknowledgment from the receiver in response to an RFID wake-up signal, the sender assumes that the receiver tag did not detect the signal or that the signal level is too low to activate the receiver tag. The sender then transmits the RFID wake-up signal again, with a maximum of three retries. If the receiver acknowledges receipt of one of the RFID wake-up signals, then the sender proceeds with the transmission. Otherwise, the sender stops its attempts to use RFID wake-up signals to this receiver.

4.2.4 TRADE-OFFS

RFID Impulse supports traffic-based selection of low-power radio modes. When the traffic load is high in a particular region of the network, nodes use lighter sleep modes as they have to wake up frequently to send and receive packets. When the traffic load is low in a particular region of the network, switching between sleep and active states is less frequent, so nodes use deeper sleep modes that provide the highest energy savings. Determining quantitative thresholds for optimal sleep mode selection demands an energy model that captures all components contributing to energy consumption at sensor nodes.

4.3 ENERGYANALYTICAL MODEL

In order to model the energy consumption of the three MAC protocols, considers all the energy components that contribute to the overall energy consumption at a node including sensor and the radio.

Consider a converge-cast application where all nodes sample their sensor periodically and send the data toward the base station. Here focuses on energy consumption during a single sampling period.

4.3.1 LISTENING ENERGY

Listening energy is the radio energy consumption at the time when the radio is active but not receiving or sending any packets and given by equation 4.1

$$E_l^{lpl} = \frac{S}{CK} * T_{CH} * I_{listen} * V \qquad 4.1$$

Where the notations are illustrated in the table given below:

TABLE I

Notations	Parameter
E_l^{lpl}	Listening energy
S	The sampling period
CK	Check interval
T_{CH}	Time during which the node is awake every cycle
I_{listen}	Current draw of the radio in listening mode
V	Number of times the node spend in idle

4.3.2 SWITCHING ENERGY

The switching energy [29] is the energy consumption for switching the radio state between states, including normal, power down, and idle modes. The energy consumed for switching the radio from sleep mode α to active mode is given by the equation 4.2

$$E_{switch}^{\propto} = \frac{(I_{active} - I_{\propto}) * T_{\propto} * V}{2} \quad \text{……………………….…………..4.2}$$

Where the notations are illustrated in the table given below:

TABLE II

Notations	Parameter
$E_{switch}^{\propto}$	Switching energy from sleep mode α to active mode
I_{active}	Current draw of the radio in active mode
$I_{\propto}$	Current draw of the radio in sleep mode α
$T_{\propto}$	Time required for the radio to go from sleep mode α to active mode
$\propto$	Sleep mode

4.3.3 TRANSMISSION ENERGY

The transmission energy is the energy consumption for transmitting packets and their associated control overhead on the radio. For any time period, the transmission energy is given by equation 4.3

$$E_t = P_{sent} * P_{length} * T_B * I_t * V \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 4.3$$

Where the notations are illustrated in the table given below:

TABLE III

Notations	**Parameter**
E_t	Transmission energy
P_{length}	Length of a packet in a bytes
T_B	Time for sending 1 byte over the radio
I_t	Current draw of the radio while in transmit mode

4.3.4 RECEIVING ENERGY

The receiving energy is the energy consumption while receiving packets and their associated control overhead on the radio. For any time period, the reception energy is given by equation 4.4

$$E_r = P_{recv} * P_{length} * T_B * I_r * V \ldots\ldots\ldots\ldots\ldots\ldots\ldots 4.4$$

Where I_r is the current draw of the radio while receiving.

4.3.5 SLEEPING ENERGY

The sleeping energy is simply the energy consumption, while the radio is in low-power mode. The given equation 4.5, evaluates the sleeping energy for a node that goes into sleep mode α when it is off:

$$E_{sleep} = T_{rf}^{off} * I_{\propto} * V \quad \text{.........} 4.5$$

4.3.6 SENSING ENERGY

Every sensor node includes several physical sensors, from simple temperature sensors to complex video sensors. These sensors will have their own energy consumption characteristics, and in some case, their own sampling frequency. The energy consumption of a sensor i is given by equation 4.6

$$E_s^i = T_i * I_i * V \quad \text{.........} 4.6$$

So the energy consumption for all the sensors attached to a node is given by equation 4.7

$$E_s = \sum_{i=1}^{N} \left[E_s^i * \frac{S}{S_i} \right] \quad \text{.........} 4.7$$

If all the sensors have the same sampling period S as the node then energy consumption for all the sensors attached to a node is given by equation 4.8

$$E_s = \sum_{i=1}^{N} E_s^i \quad \text{.........} 4.8$$

Where the notations are illustrated in the table given in TABLE IV:

TABLE IV

Notations	**Parameter**
E_s^i	Sensing energy for a sensor i
E_s	Overall energy of all the sensors
T_i	Time required for obtaining a single

	sample from sensor i
I_i	Current draw of sensor i
N	Number of sensors attached to the node
S	Sampling period
S_i	Specific sampling period for sensor i

4.3.7 OVERALL ENERGY

The sum of all the above energy consumption equations 4.1 to 4.8 gives the whole energy consumption at each node and is given by equation 4.9

$$E_P^{\propto} = E_l + E_{switch} + E_t + E_r + E_{sleep} + E_s \ldots\ldots\ldots\ldots\ldots 4.9$$

Hence we compute the energy optimize MAC protocol (That is lowest energy consumption) for a given network scenario.

4.3.8 DELAY

Use different low-power radio modes on the end to end delay. We assume delay $T_{\propto}$ for sleep mode$\propto$, T_t the packet transmission time, T_{bo} the back of time,T_q queuing delay. Then the packet transmission time is given by the equation 4.10

$$T_t = T_B * P_{length} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 4.10$$

And the back of time is given by equation 4.11

$$T_{bo} = T_B * 54 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 4.11$$

in a highly congested scenario for IEEE802.15.4 radios.

Chapter 5

IMPLEMENTATION DETAILS AND SIMULATION RESULTS

5.1 NETWORK SIMULATOR USED

Network simulator (version 2) [32, 33, 34] is an object-oriented, discrete event driven network simulator developed at UC Berkeley. It is written in C++ and uses OTcl (Tcl script language with Object-oriented extensions developed at MIT) as a command and configuration interface. *ns v2* has three substantial changes from *ns v1*:

1. More complex objects in *ns v1* have been decomposed into simpler components for greater flexibility.
2. The configuration interface is now OTcl, which is an object oriented version of Tcl.
3. The interface code to the OTcl interpreter is separated from the main simulator.

Fig.5.1 shows the simplified user's view of *ns*. *ns* is an Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler, network component object libraries, and network setup module libraries. To setup and run a simulation network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using network objects and setup functions in the library, and tells the traffic sources when to start and stop transmitting packets through the event scheduler.

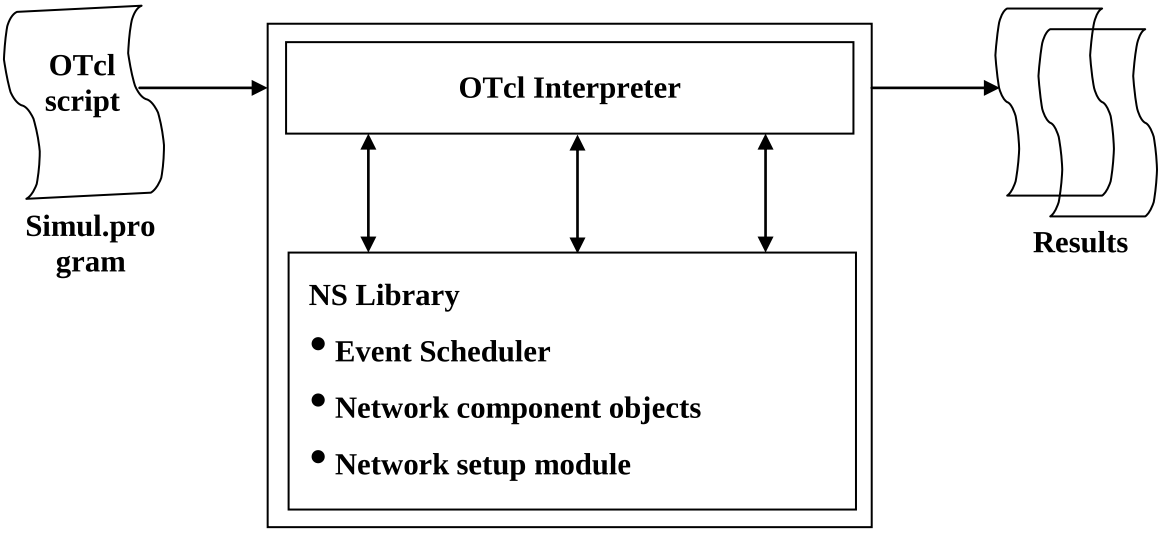

Fig. 5.1: Simplified User's View

For obtaining *ns* simulation results, when our simulation is finished (from *fig. 5.1*), *ns* produces one or more text-based output files which contain detailed simulation data, if specified in OTcl script. This data can be used for simulation analysis or as an input to the graphical simulation display tool called Network Animator (NAM).

5.2 ENERGY ANALYSIS MODEL

To support the simulation of our Energy optimization MAC (EO-MAC) protocol, we have study the energy analysis model. Energy model is a node attribute that has an initial value which represents the level of energy, the node has at the beginning of the simulation; known as *initial Energy_*. It also has given energy usage for every packet it transmits and receives, known as *txPower_* and *rxPower_* respectively.

The energy model is used through the node configuration API which consists of the type of addressing structure used in the simulation, defining the network components **for mobile nodes**, turning on/off trace options at Agent/Router/MAC levels, selecting the type of adhoc routing protocol wireless nodes or defining their energy model. The detailed TCL script used to simulate our model is given below.

```
# Simulation of Energy consumption and through

set opt(chan)                Channel/WirelessChannel
set opt(prop)                Propagation/TwoRayGround
set opt(netif)               Phy/WirelessPhy
#set opt(mac)           Mac/802_15_4                ;# MAC type
#set opt(mac)           Mac/RFID               ;# MAC type
set opt(mac)           Mac/DMAC                ;# MAC type
set opt(ifq)                 Queue/DropTail/PriQueue
set opt(ll)                  LL
set opt(ant)           Antenna/OmniAntenna
set opt(x)                   800       ;# X dimension of the topography
set opt(y)                   800              ;# Y dimension of the topography
set opt(cp)                  "../mobility/scene/cbr-50-10-4-512"
set opt(sc)                  "../mobility/scene/scen-670x670-50-600-20-0"

set opt(ifqlen)              50               ;# max packet in ifq
set opt(nn)                  2                ;# number of nodes
set opt(seed)                0.0
set opt(stop)                700.0            ;# simulation time
set opt(tr)                  MyTest.tr        ;# trace file
set opt(nam)                 MyTest.nam       ;# animation file
set opt(rp)            DumbAgent       ;# routing protocol script
set opt(lm)            "off"          ;# log movement
set opt(agent)         Agent/DSDV
set opt(energymodel)    EnergyModel     ;
#set opt(energymodel)    RadioModel     ;
set opt(radiomodel)       RadioModel    ;
set opt(initialenergy)  1000           ;# Initial energy in Joules
#set opt(logenergy)      "on"          ;# log energy every 150 seconds


Mac/SMAC set syncFlag_ 1

Mac/SMAC set dutyCycle_ 10

set ns_             [new Simulator]
set topo [new Topography]
set tracefd         [open $opt(tr) w]
set namtrace    [open $opt(nam) w]
set prop [new $opt(prop)]

$topoload_flatgrid $opt(x) $opt(y)
ns-random 1.0
$ns_ trace-all $tracefd
#$ns_ namtrace-all-wireless $namtrace 500 500

#
# Create god
#
create-god $opt(nn)


#global node setting
```

```
	$ns_ node-config -adhocRoutingDumbAgent \
				-llType $opt(ll) \
				-macType $opt(mac) \
				-ifqType $opt(ifq) \
				-ifqLen $opt(ifqlen) \
				-antType $opt(ant) \
				-propType $opt(prop) \
				-phyType $opt(netif) \
				-channelType $opt(chan) \
				-topoInstance $topo \
				-agentTrace ON \
				-routerTrace ON \
				-macTrace ON \
				-energyModel $opt(energymodel) \
				-idlePower 1.0 \
				-rxPower 1.0 \
				-txPower 1.0 \
			-sleepPower 0.001 \
			-transitionPower 0.2 \
			-transitionTime 0.005 \
				-initialEnergy $opt(initialenergy)



	$ns_ set WirelessNewTrace_ ON
#set AgentTrace				ON
#set RouterTrace			OFF
#set MacTrace				ON

	for {set i 0} {$i < $opt(nn) } {incr i} {
		set node_($i) [$ns_ node]
		$node_($i) random-motion 0		;# disable random motion
	}

#	$node_(1) set agentTrace ON
#	$node_(1) set macTrace ON
#	$node_(1) set routerTrace ON
#	$node_(0) set macTrace ON
#	$node_(0) set agentTrace ON
#	$node_(0) set routerTrace ON

set udp_(0) [new Agent/UDP]
$ns_ attach-agent $node_(0) $udp_(0)
set null_(0) [new Agent/Null]
$ns_ attach-agent $node_(1) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 512
$cbr_(0) set interval_ 10.0
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 50000
$cbr_(0) attach-agent $udp_(0)
$ns_ connect $udp_(0) $null_(0)
```

```
$ns_ at 1.00 "$cbr_(0) start"
#$ns_ at 177.000                    "$node_(0) set ifqLen"


#
# Tell all the nodes when the simulation ends
#
for {set i 0} {$i < $opt(nn) } {incr i} {
   $ns_ at $opt(stop) "$node_($i) reset";
}
$ns_ at $opt(stop) "puts \"NS EXITING...\" ; $ns_ halt"

set b [$node_(0) set mac_(0)]
#set c [$b set freq_]
set d [Mac/SMAC set syncFlag_]

#set e [$node_(0) set netif_(0)]

#set c [$e set L_]
set c [Mac/SMAC set dutyCycle_]
#puts $tracefd "M 0.0 nn $opt(nn) x $opt(x) y $opt(y) rp $opt(rp)"
#puts $tracefd "M 0.0 sc $opt(sc) cp $opt(cp) seed $opt(seed)"
#puts $tracefd "M 0.0 prop $opt(prop) ant $opt(ant)"
#puts $tracefd "V $b : $c : $d :"
puts "Starting Simulation..."
$ns_ run
```

5.3 SIMULATION AND RESULTS

A detail of simulation methodology used for our proposed EO-MAC protocol is explained in below sections:

5.3.1 SIMULATION ENVIRONMENT

We have used *ns2* as a simulation tool to evaluate the performance of our proposed algorithm under different varying time intervals i.e. 0, 50,100, 150, 200, 250, 300, 350 and cbr intervals i.e., 1.0, 1.5, 2.0, 2.5, 3.0, 3.5, 4.0, 4.5, 5.0. In our simulation, nodes are spread in a terrain of 800×800. The nodes are randomly deployed within the simulation area. Each node has same 22 meters of transmission range.

Results of simulation are expressed using following metrics:

- Energy Consumption
- Throughput

Energy Consumption is expressed in terms of total energy consumed by all the nodes in the transmission as well as in the reception of the packets.

Throughput is defined as the ratio of total packets sent per second (packets/s).

5.3.2 SIMUALTION PARAMETERS

The simulation parameters are summarized in below table:

TABLE VI: SIMULATION PARAMETERS

Parameters Name	Values
ns2 version	2.33
Simulation time	700 seconds
Traffic	cbr
Routing Protocol	DSDV
Transmission range	22 meters
Transmitting and receiving antenna height	1.5 meters
Bandwidth	11 Mb
Minimum transmission power	0.031622777 W
Carrier sense power	5.011872e-12 W
Receive power threshold	5.82587e-09 W
Initial Energy	1000 Joule

5.4 RESULTS AND ANALYSIS

The results are obtained in terms of two metrics i.e., energy consumption and throughput are represented in the form of graphs, which are then compared and justified.

5.5.1 ANALYSIS OF ENERGY CONSUMPTION GRAPH

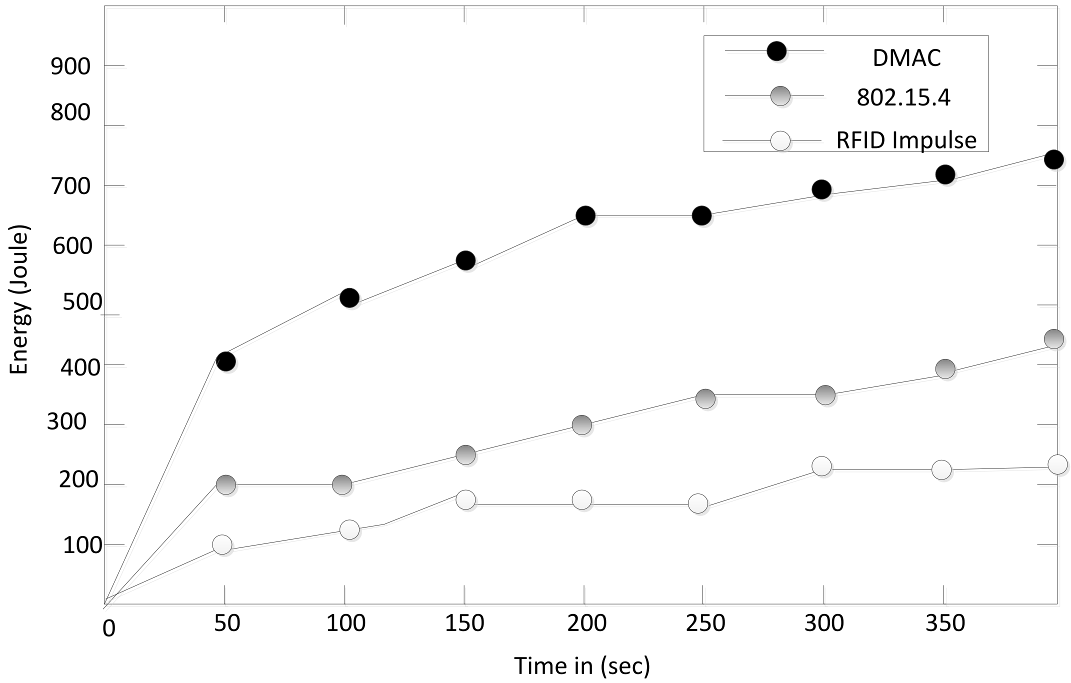

Fig. 5.2: Comparison of energy consumption

Fig. 5.2 shows the node energy consumption (mJ) versus time interval (s) for RFID Impulse, IEE802.15.4 and DMAC Protocols is plotted by varying the time interval which impact the traffic load on the source node. For this experiment, each node has initially 1000 Joules of energy. The figure indicates that our proposed energy optimization MAC (EO-MAC) protocol that is RFID Impulse presents an improvement over IEEE802.15.4 and DMAC protocol, which can be explained by the use of minimum transmission power required for transmitting DATA and ACK packets.

5.5.2 ANALYSIS OF THROUGHPUT GRAPH

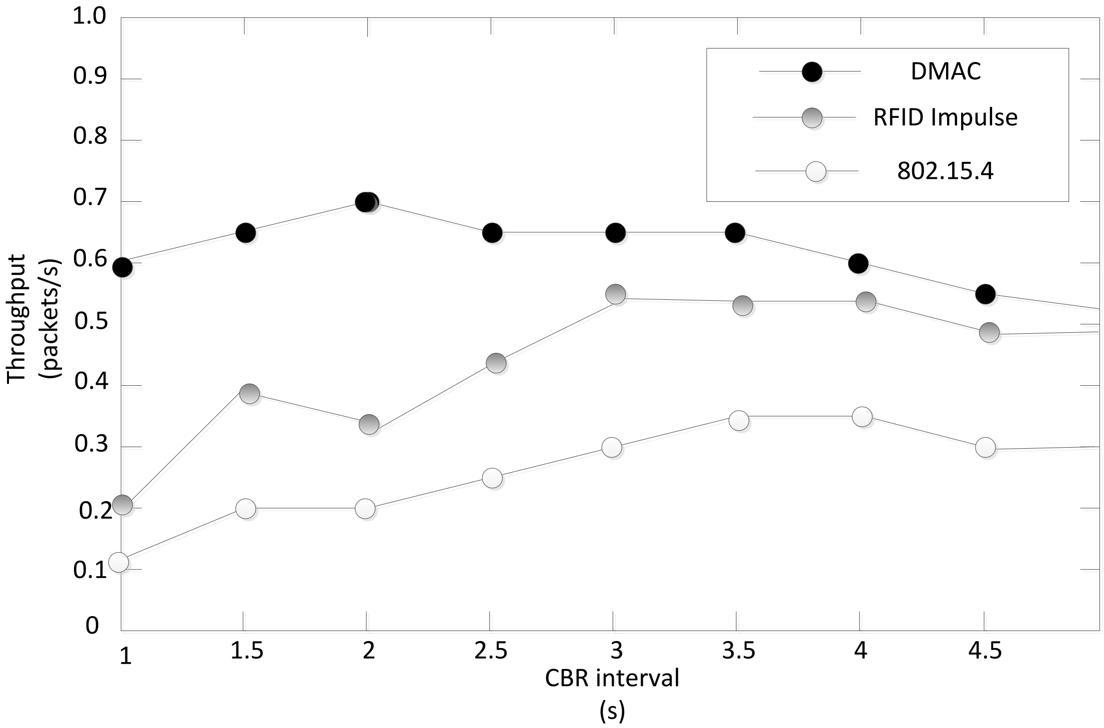

Fig. 5.3: Throughput comparison

Another important parameter is the network throughput. Fig. 5.3 shows that the throughput of RFID Impulse is greater than the IEE802.15.4 but lower than the DMAC protocol. Initially from 1.0 to 3.0 cbr interval, throughput of EO-MAC is better than DMAC and IEEE 802.15.4. Although, after 3.0 cbrinterval,the throughput of EO-MAC protocol is slowly decreasing as CBR interval increases. However, overall throughput of it is improved.

As described above, compared to the IEE802.15.4 and DMAC protocol, our proposed EO-MAC protocol i.e. RFID Impulse has improved the energy consumption and competes with DMAC in terms of throughput of the networks. Thus, RFID Impulse improves the overall energy performance.

Chapter 6

CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

Basically wireless sensor networks must be designed with keeping energy efficiency in mind. So many protocols have been developed for energy efficiency, but no one can actually fulfill the changing application needs. The adaptive radio sleeps modes as an energy optimization technique has been used. Because nearly all sensor networks MAC protocol alternate frequently between sleep and awake states, the frequency of this state switching should dictate the appropriate sleep mode that minimizes energy consumption.

We proposed an energy optimization MAC (EO-MAC) protocol, which is based on adaptive radio low-power sleep modes with current traffic conditions in the network. We proposed an analytical model for energy consumption. In this analytical model, a comparative study for energy consumption of different MAC protocols (DMAC, and IEEE802.15.4) has been studied.

The queuing and collision back off delay are higher at critical nodes near the base station. But when the nodes use adaptive sleep modes then they select light sleep for their higher forwarding load which minimizes$T_{\propto}$, and hence reduces the end-to-end delay for the packets these nodes forward.

We have studied the proposed Energy Optimization MAC (EO-MAC) protocol by energy analysis model for three protocols IEE802.15.4, D-MAC and RFID impulse. The proposed model is simulated using ns2. The comparative analysis of these three protocols show that RFID impulse with adaptive low power mode gives lower energy consumption than the IEEE802.15.4 and D-MAC protocol that is RFID impulse with adaptive low power mode achieves more energy saving and higher throughput.

6.2 FUTURE WORK

An interesting direction for future work is to implement RFID Impulse by

- attaching RFID tags to the2external interrupt pin of sensor node microcontroller units (MCUs), and then,
- Configuring the radio to trigger the remote tags.

References

[1] A. J. Goldsmith and S. B. Wicker , “ Design challenges for energy - constrained ad hoc wireless networks ” , *IEEE Wireless Communications* , vol. 9 , no. 4 , Aug. 2002 , pp. 8 – 27 .

[2] C. Herring and S. Kaplan , “ Component - based software systems for smart environments ” , *IEEE Personal Communications* , vol. 7 , no. 5 , Oct. 2000 , pp. 60 – 61.

[3] D. Trossen and D. Pavel , “ Sensor networks, wearable computing, and healthcare Applications ” , *IEEE Pervasive Computing* , vol. 6 , no. 2 , Apr. – June 2007 , pp. 58 – 61 .

[4] I. F. Akyildiz , W. Su , Y. Sankarasubramaniam , and E. Cayirci , “ Wireless sensor networks: A survey ”, *Computer Networks* , vol. 38 , no. 4 , Mar. 2002 , pp. 393 – 422 .

[5] R. Jafari , A. Encarnacao , A. Zahoory , F. Dabiri , H. Noshadi , and M. Sarrafzadeh , “ Wireless sensor networks for health monitoring ” , in *Proceedings of 2nd AnnualInternational Conference on Mobile and Ubiquitous Systems: Networking andServices (MobiQuitous ’ 05)* , July 2005 , pp. 479 – 481 .

[6]C. Shiva Ram Murthy, and B. S. Manoj, “Ad-hoc Wireless Networks: Architectures and protocols,” Copyright © 2004 by Pearson education, Inc.

[7]S. S. Kulkarni, “TDMA Services for Sensor Networks,” Proc. 24th Int’l. Conf.Distrib. Comp. Sys. Wksps., Mar. 2004, pp. 604-09.

[8] Wei Ye, John Heidmann, “Medium Access Control in Wireless Sensor Networks” USC/ISI TECHNICAL REPORT ISI-TR-580, OCTOBER 2003.

[9] I. Demirkol, C. Ersoy, F. Alagoz. “MAC protocols for Wireless Sensor Networks: A Survey” IEEE communication magazine, pages 115-121, April 2006.

[10] KoenLangendoen, “Medium access control in wireless sensor networks,” Vol. II: Practice and Standards edited by H. Wu and Y. Pan, published by Nova Science Publishers © 2007.

[11] P. Naik, K. Sivalingam, “A Survey of MAC Protocols for Wireless Sensor Networks,” in: C. Raghavendra, K. Sivalingam, T. Znati (Eds.), Wireless Sensor Networks, Kluwer Academic Publishers, 2004.

[12] W. Ye, J. Heidemann, and D. Estrin, “An energy efficient MAC protocol for Wireless Sensor Networks,” in Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM 2002), New York, USA, June 2002, pp. 1567-1576.

[13] IEEE 802.11, Wireless LAN media access control (MAC) and physical layer (PHY) specifications, 1999.

[14] W. Ye, J. Heidemann, and D. Estrin, “Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks,” in IEEE/ACM Transactions on Networking, June 2004, pp. 493-506.

[15]J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for sensor networks” in Proceedings of 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys), November 3-5, 2004.

[16] M. Buettner, G. V. Yee, E. Anderson, and R. Han, “X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks” in Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys 2006), Boulder, Colorado, USA, 2006, pp. 307-320.

[17] T. V. Dam, and K. Langendoen, “An adaptive energy-efficient MAC protocol for wireless sensor networks” in 1st ACM Conf. n Embedded Networked Sensor Systems (SenSys 2003), Los Angeles, CA, Nov. 2003, pp. 171-180.

[18] V. Rajendran, K. Obraczka, and Garcia-Luna-Aceves, “Energy-Efficient, Collision-Free Medium Access Control for Wireless Sensor Networks” in Proceedings of ACM SenSys 03, Los Angeles, CA, November 2003.

[19] L. V. Hoesel, and P. Havinga, “A lightweight medium access protocol (LMAC) for wireless sensor networks” in Proceedings of 1st International Workshop on Networked Sensing Systems (INSS 2004), Japan, June 2004.

[20] S. Chatterjea, L. V. Hoesel, and P. Havinga, "AI-LMAC: an adaptive, Information-centric and lightweight MAC protocol for wireless sensor networks" in Proceedings of 2nd International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2004), Melbourne, Australia, December 2004.

[21]I. Riiee, A. Warrier, M. Aia, and J. Min, "Z-MAC: A hybrid MAC for wireless sensor networks," in 3rd ACM Conf. on Embedded Networked Sensor Systems (SenSys 2005), San Diego, CA, Nov. 2005, pp. 90-101.

[22] T. Zheng, S. Radhakrishnan, and V. Sarangan, "PMAC: An adaptive energy-efficient MAC protocol for wireless sensor networks," in 19th IEEE Int. Parallel and Distributed Processing Symposium (IPDPS 2005), Denver, CO, Apr. 2005.

[23] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on SystemSciences (HICSS '00)*, Maui, USA, vol. 2,pp. 3005–3014, January 2000.

[24] Institute of Electrical and Electronics Engineers, Inc., ''IEEE Std. 802.15.4-2003: Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (LR-WPANs)" , New York, IEEE Press. Oct. 1, 2003

[25] R. Jurdak, A.G. Ruzzelli, and G.M.P. O'Hare, "Adaptive Radio Modes in Sensor Networks: How Deep to Sleep?" Proc. IEEE Comm. Soc. Conf. Ad Hoc and Sensor Networks (SECON '08), June 2008.

[26] J. Polastre, J. Hill, and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," Proc. ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '04), 2004.

[27] A.G. Ruzzelli, G.M.P O'Hare, and R. Jurdak,"MERLIN: Cross-Layer Integration of MAC and Routing for Low Duty-Cycle Sensor Networks," Ad Hoc Networks J., vol. 6, no. 8, pp. 1238- 1257,Feb. 2008.

[28] L. Gu and J.A. Stankovic, "Radio-Triggered Wake-Up Capability for Sensor Networks," Proc. 10th IEEE Real-Time and Embedded Technology and Applications Symp., 2004.

[29] A.G. Ruzzelli, R. Jurdak, and G.M.P. O'Hare, "On the RFID Wake-Up Impulse for Multi-Hop Sensor Networks," Proc. Convergence of RFID and Wireless Sensor Networks and Their Applications (SenseID) Workshop at ACM Int'l Conf. Embedded Networked Sensor Systems (Sensys '07), Nov. 2007.

[30] A.G. Ruzzelli, P. Cotan, G.M.P. O'Hare, R. Tynan, and P.J.M Havinga, "Protocol Assessment Issues in Low Duty Cycle Sensor Networks: The Switching Energy," Proc. IEEE Int'l Conf. Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06), June 2006.

[31] G. Lu B. Krishnamachari, and C. S. Raghavendra, ''An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks" , in Proceedings of 18th International Parallel and Distributed Processing Symposium(IPDPS'04), Santa Fe, NM, Apr.2004, pp. 224-231.

[32] *ns2*mannual, http://www.isi.edu/nsnam/ns/ns-documentation.html.

[33] Jae Chung, and Mark Claypool, "ns by example" http://nile.wpi.edu/NS/.

[34] Marc Greis, "ns tutorial" http://www.isi.edu/nsnam/ns/tutorial.

[35] http://www.isi.edu/ilense/software/smac/ns2_energy.

[36] P.Gupta and P.R.Kumar, Critical power for asymptotic connectivity in wireless network. Stochastic Anylysis, Control, Optimization and Applications:A Volume in Honor of W.H.Flerning,pp.547-566.Boston, MA: Birkhauser, March1998

[37] A. Cerpa et al., "Habitat monitoring: Application driver for wireless communications technology,"2001 ACM SIGCOMM Workshop on Data Communications in Latin America and theCaribbean, Costa Rica, April 2001.

[38] G.J. Pottie, W.J. Kaiser, "Wireless IntegratedNetwork Sensors," Communications of the ACM,vol. 43, no. 5, pp. 551-8, May 2000.

[39] J. Warrior, "Smart Sensor Networks of the Future,"Sensors Magazine, March1997.

[40] Raja Jurdak, Member, IEEE, Antonio G. Ruzzelli, and Gregory M.P. O'Hare "Radio Sleep Mode Optimization in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 9, No. 7, July 2010.

[41] Jun Zheng, Abbas jamalipour, "Wireless Sensor Networks: A network prospective", A john Willey & sons, Inc. publication, pp. 1-150.

ABBREVIATIONS

ACK	Acknowledgment
cbr	Constant Bit Rate
CSMA	Carrier Sense Multiple Access
CSMA/CA	CSMA with Collision Avoidance
CTS	Clear-to-Send
DIFS	Defer Inter-Frame Spacing
DSDV	Distance Sequenced Distance-Vector
EO-MAC	Energy-Optimization Medium Access Control
EIFS	Extended Inter-Frame Spacing
FDMA	Frequency Division Multiple Access
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter-Frame Spacing
LAN	Local Area Network
MAC	Medium Access Control
MACA	Multiple Access Collision Avoidance
MIT	
NAV	Network Allocation Vector
QoS	Quality of Service
RSSI	Received Signal Strength Indicator
RTS	Request-To-Send
SIFS	Short IFS
S-MAC	Sensor-MAC
SYNC	Synchronization
SYNC-REC	Synchronization-Receive
TDMA	Time Division Multiple Access
TPC	Transmission Power Control

WLAN	Wireless LAN
WSN	Wireless Sensor Network

APPENDIX

set ns_ [new simulator]

This command is creates an instance of the simulator object.

$ns_ node

This command is used to create a simple node. This returns a handle to the node instance created.

$topoload_flatgrid<X><Y><optional:res>

This initializes the grid for the topology object. <X> and <Y> are the x-y co-ordinates for the topology and are used for sizing the grid. The grid resolution may be passed as <res> whose default value is 1.

$ns_ trace-all <tracefile>

This command is used to set up tracing in ns. All traces are written in the <tracefile>.

create-god<num_nodes>

This command is used to create a God instance. The number of mobile nodes is passed as argument which is used by God to create a matrix to store connectivity information of the topology.

$ns_ node-config -<config-parameter><optional-value>

This command is used to configure nodes. The different config-parameters are addressingType, different type of the network stack components, whether tracing will be turned on or not, mobileIP flag is turned on or not, energy model is being used or not, etc.

set udp0 [newAgent/UDP]

This command creates an instance of the UDP agent.

set cbr1 [newApplication/Traffic/CBR]

This command creates an instance of the CBR traffic.

$node attach-agent <node><agent>

This command attaches the <agent> to the <node>. Here we assume that the <agent> has already been created. An agent is typically been created by *set agent [new Agent/AgentType]* where Agent/AgentType defines the class definition of the specified agent type.

$ns_ connect <src><dst>

Sets up a connection between the src and dst agents.

$ns_ run

This command starts the simulator.