A Performance Analysis of Wireless Sensor Networks

by

Hao Gu

A Thesis
in
the Department
of
Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Applied Science (Electrical Engineering) at
Concordia University
Montreal, Quebec, Canada

April, 2006

Your file Votre référence
ISBN: 978-0-494-20747-5
Our file Notre référence
ISBN: 978-0-494-20747-5

ABSTRACT

A Performance Analysis of Wireless Sensor Networks

Hao Gu

Wireless Sensor Networks (WSNs) are expected to be the next technology to have a huge impact on society. WSNs consist of a large number of tiny sensors which integrate sensing, processing and wireless communication capabilities. Research on all aspects of WSN has been gaining momentum very rapidly in the last few years. An important issue is the choice of MAC protocol for WSN. The proposed MAC protocols may be divided into two major categories: contention and scheduling based. Contention based protocols consume more energy than scheduling based protocols because of retransmission of messages caused by collisions. However, scheduling based protocols, i.e. TDMA requires a large amount of resources because each customer is assigned a timeslot. In order to save both resources and energy, a TDMA media access protocol with slot reuse had been proposed in this work, we consider modeling of such a wireless sensor network. It is assumed that the nodes have two modes of operation, active and sleep modes. We model the sensor network as a Jackson network with node breakdowns. We determine the joint distribution of the queue lengths in the sensor network. From this result, we derive the probability distribution of the number of active nodes and blocking probability of node activation. Then, we present the mean packet delay, average sleep period of a node as well as the network throughput. The model also captures reduction in the traffic load due to elimination of redundant information in the collected data. Finally, we discuss how the derived results may be used in the design of sensor networks.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Mustafa K. Mehmet Ali for his excellent guidance and advice through the years. Undoubtedly, the research work that I can successfully finish was benefited from his talent and financial support. I am extremely grateful for his patient, support and friendly.

Special thanks go to all the professors who taught me courses, which have been profoundly used in my later research.

Last but not the least, I would like to give my deepest appreciation to my parents, sister and all the family members of my aunt's for their love and support, and also many thanks to my friends in Montreal, Toronto and Vancouver.

Hao Gu

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

Symbol	Definition
λ_j	the external arrival rate to node j
μ_j	the service intensity at node j
$r(i, j)$	the transition probability from node i to node j
n_j	the number of customers at node j, $j \in \bar{J}$
e_j	the total arrival rate of the customers to node j (including internal and external rate)
$\mathbf{e} = [e_1, e_2, ..., e_J]$	the vector of total arrival rate of the J customers
$\boldsymbol{\lambda} = [\lambda_1, \lambda_2, ..., \lambda_J]$	the vector of the external arrival rate of the J customers
$\mathbf{R}$	the matrix of transition probability of noe i to node j
$\rho_j = e_j / \mu_j$	utilization of node j
$\boldsymbol{n} = [n_1, n_2, ..., n_J]$	the joint queue length vector
$\pi(n_1, n_2, ..., n_J)$	the joint probability distribution of queue length vector
$\bar{J}^* = \{0 \cup \bar{J}\}$	the augmented node set that also includes node 0 which denotes departures from the network
$\tilde{r}(i, j)$	the transition probability from node i to node j with nodes breakdown and repair processes
$\bar{I}_U$	the set of the nodes in the up status
$\bar{I}_D$	the set of the nodes in down status
$\bar{I}_U^* = \{\bar{I}_U \cup 0\}$	the set of nodes in the up status including 0 node in the up status

$a_i(n_i)$	the breakdown rate of node i with local load n_i when in the up status
$b_i(n_i)$	the repair rate of node i with local load n_i when in the down status
$A\ (n_i : i \in \overline{I}_U)$	the breakdown intensities of the network at state $\boldsymbol{n}$
$B\ (n_i : i \in \overline{I}_D)$	the repair intensities of the network at state $\boldsymbol{n}$
α	the breakdown rate of the empty node
β	the repair rate of the node
$\lvert\overline{I}_U\rvert$	the number of nodes in sets $\overline{I}_U$
$\lvert\overline{I}_D\rvert$	the number of nodes in sets $\overline{I}_D$
C	the normalization constant of Jackson network with unreliable nodes
E	the total state space of the joint queue length vector of the Jackson network
$\overline{M}_j$	the set of the nodes within the transmission range of node j
$r_{\max}$	the number of slots in a frame
Ω_U	the set of network states where all nodes are in the up status
Ω_D	the set of network states where at least one node is in down status
$\overline{\pi}(\boldsymbol{n})$, $\overline{\pi}(\overline{I}_D, \boldsymbol{n})$	the sensor network queue length distribution in a truncated state space
G	the normalization constant of Jackson network with unreliable nodes in a truncated space
$q(k)$	the probability distribution of the number of active nodes

$\bar{k}$	the average number of active nodes in the system, where the number of active nodes in system is k
φ_j	the probability of node j in active status
$\bar{\varphi}$	the probability of a node in active status
$\bar{\boldsymbol{M}}_{Uj}$	the set of active nodes within the transmission range of node j at a given network state $\boldsymbol{n}$
P_j	the probability that activation of node j will be blocked
$p(n_j)$	the marginal distribution of the queue length of node j
$\bar{\boldsymbol{n}}_j$	the average queue length at node j
λ	the total external arrival rate of the packets in system
$\alpha_j(\boldsymbol{r})$	the probability that node j will experience r consecutive down periods
θ_j	the sleep duration of node j
σ	the drop rate of each sensor node
x_i	the i'th down period
S	the average throughput of the network

LIST OF ABBREVIATIONS

Abbreviation	Definition
ACK	Acknowledgment
ADC	Analog Digital Converter
ADV	Advertisement
ALERT	Automated Local Evaluation in Real Time
ARPAnet	Advanced Research Projects Agency Network
CAP	Contention Access Period
CDMA	Code Division Multiple Access
CFP	Contention Free Period
CSMA/CA	Carrier Sensor Multiple Access / Collision Avoidance
CTS	Clear-to-Send
DARPA	Defence Advanced Research Projects Agency
DSN	Distributed Sensor Network
EAR	Eavesdrop And Register algorithm
FCFS	First Come First Serve
FDMA	Frequency Division Multiple Access
FFD	Full-Function Device
GTS	Guaranteed Time Slots
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

IT	Information Technology
LEACH	Low Energy Adaptive Clustering Hierarchy
LR-WPAN	Low Rate Wireless Personal Area Network
MAC	Medium Access Control
MACA	Medium Access Collision Avoidance
MACAW	Medium Access Collision Avoidance for Wireless LAN
MANET	Mobile Ad hoc Network
MECN	Minimum Energy Communication Network
MEMS	Micro-Electro-Mechanical System
MIT	Massachusetts Institute of Technology
OSI	Open System Interconnection
PACMAN	Power Aware Computing/Communication for Mobile Ad hoc and Sensor Networks
QoS	quality of service
REQ	Request.
RFD	Reduced-Function Device
RTS	Request-to-Send
SCADDS	Scalable Coordination Architectures for deeply Distributed and Dynamic Systems
SINA	Sensor Information Networking Architecture
S-MAC	Sensor Medium Access Control

SMACS	Self-organizing Medium Access Control for Sensor Networks
SMECN	Small Minimum Energy Communication Network
SOSUS	Sound Surveillance System
SPIN	Sensor Protocols for Information via Negotiation
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UCLA	University of California - Los Angeles
WINS	Wireless Integrated Network Sensors
WPAN	wireless Personal Area Network
WSN	Wireless Sensor Network
μAMPS	μ Adaptive Multi-domain Power aware Sensors

CHAPTER 1:

INTRODUCTION

1.1 Introduction

Wireless communications has been developing with a very fast pace during the last two decades. It has enabled the mobile users to have the same services that wired communications has been providing to the stationary users. Mobile users have access to voice communications, Internet, and remote control of electrical devices. Thus, society is immensely benefiting from the innovative wireless technologies such as Bluetooth, Wireless Personal Area Network (WPAN), etc. Among the latest to emerge is wireless sensor networks.

A wireless sensor network (WSN) consists of a large number of tiny sensor nodes, which self-organize themselves into a communications network. The prosperous development in wireless communications, micro-electro-mechanical system (MEMS) technologies, and digital electronics made the low-cost, low-power and multifunctional sensor nodes feasible **[1]**. Sensor nodes are small devices that integrate sensing, processing and wireless communications capabilities. Since the nodes have limited computational capability, the collected data needs to be forwarded to a sink where the processing of information takes place. Sensor nodes may be far away from the sink due to their limited transmission range. Thus, the information may need to be delivered to the sink through multihop communications with intermediate nodes acting as relays. Therefore, sensor nodes are both source of information as well as they take part in delivery of the information to the final destination. As a result, sensor nodes have both transmitter and receiver functions though not simultaneously.

Sensor nodes are expected to cost very little and this will enable their large scale deployment. High density sensor networks may have millions of nodes. Wireless sensor networks have huge potential for applications in automation of building, utilities, industrial, home, shipboard, and transportation systems [2]. Next, we describe the various applications of wireless sensor networks [3].

1) Environmental applications

- Tracking the movements of endangered animals, and monitoring the environment on earth.
- Forest fire detection, because of densely deployment of sensor nodes, they could report the original location of the fire to the user before the fire is spread uncontrollable.
- Flood detection, weather sensors may send the information to the ALERT system [4] which analyses the data to determine the intensity of flood according to the rainfall and water levels.
- Monitoring the agricultural pesticide level in the drinking water, the level of soil erosion, and the level of air pollution.

2) Health applications

- Tracking and monitoring doctors and patients inside a hospital. For example, different sensors could be attached to the different patients for specific uses such as detecting the heart rate, or blood pressure.
- Providing an interface to the disabled to help them act.

3) Home applications

- Smart environment, sensor nodes can be buried into the appliances in order to give the end users local and remote control of these appliances via the Internet.

4) Commercial applications

- Environmental control in office buildings. For example, monitoring of temperature in different places in an office building.
- Detecting and monitoring car thefts
- Vehicle tracking and detection

5) Military applications

The first applications of sensor networks were developed in DARPA for the US Department of Defence. Thus, there are many military applications of sensor networks. Such as,

- Separating the friendly force and the enemy by equipping the soldiers, equipment, and ammunition with sensor nodes.
- Battlefield surveillance of activities of the opposing forces, which may enable the commander to develop new plans.
- Targeting during battle by incorporation of sensor nodes into guidance systems of the ammunition.
- Nuclear, biological and chemical attack detection and reconnaissance

The most important characteristics of wireless sensor network nodes are,

- Low cost
- Low power
- Small size
- Short transmission distance
- Multifunctional sensor nodes
- Fault tolerance
- High density deployment
- Multihop routing

Wireless sensor networks share many characteristics with another technology, wireless ad hoc networks, which are networks without infrastructure. The common characteristics are listed below,

- The transmission range is limited, which is related to the power of signals.
- All the nodes share the same media to transmit the information.
- The signal is not protected so it is easy to intercept and be interfered by other signals in the transmission.
- The reliability of wireless transmission is not as good as that of the wired transmission.
- The network topology is dynamic.

Although wireless sensor networks are very similar to the wireless ad hoc networks, the most protocols and algorithms of ad hoc networks are not suitable for the requirements of wireless sensor networks because of the following reasons,

- The number of sensors in a sensor network can be several orders of magnitude higher than that in an ad hoc network.
- The density of sensor nodes may be very high.
- Sensor nodes are prone to failure.
- Sensor nodes in a wireless sensor network mainly use broadcast communication, while those in an ad hoc network may use point-to-point communication.
- Sensor nodes are limited in power, computational capability, and memory.

Because of their unique characteristics, we have to consider many factors in the design of wireless sensor networks such as fault tolerance, scalability, operating environment, network topology, energy efficiency, and etc.

1.2 Research Objectives and Contributions of the Thesis

It has been only a short number of years that wireless sensor networks have emerged and many issues concerning them are still under investigation including MAC, routing, and network protocols. The specification of these protocols will determine the design process of these networks as well as how they will function. Since the performance of these protocols will affect the design choices, their performance modeling is very important. Though there are various efforts to model power consumption, the other areas lack behind. The objective of this thesis has been to study the performance of MAC protocol for WSNs and consider its design implications.

There are two groups of contending MAC protocols, scheduling and contention based protocols. The TDMA forms the basis of scheduling based protocols and we choose to investigate the performance of this protocol under WSN. This performance modeling is complicated by the fact that the sensor nodes relinquish their assigned bandwidth during periods of inactivity for energy efficiency. We model WSN as a queuing network with node breakdown and we make use of recent results that appeared in the literature about this problem.

However, the application of these results poses two problems that the sensor networks have finite instead of infinite state space and blocking of node activation. Following the resolution of these problems, we determine the joint distribution of the queue lengths in the wireless sensor network. Then we derive several performance measures: probability distribution of the number of active nodes, blocking probability of node activation, average sleep period of a node, mean packet delay and network throughput.

1.3 Organization of the thesis

The thesis is organized as follows:

Chapter 1 *Introduction* presents the basic concept of the wireless sensor networks, the purpose of the study and the organization of the thesis.

Chapter 2 *Architecture of Wireless Sensor Networks* presents the background knowledge on the WSNs, and give a literature survey of the field.

Chapter 3 *Modeling of sensor networks* begins with a discussion of Jackson type of open network of queues, then introduces Jackson's network with unreliable nodes. This is followed with modeling of wireless sensor networks with Jackson type of networks and the derivation of performance measures.

Chapter 4 *Numerical Results* presents results about a 16-node sensor network with and without packet drop.

Chapter 5 *Conclusions* presents main conclusions of the thesis and future challenges.

CHAPTER 2:

ARCHITECTURE OF WIRELESS SENSOR NETWORKS

2.1 Introduction

In this chapter, we explain architecture of wireless sensor networks. First, we describe evolution of WSNs, and discuss important current research projects. Then, we present protocol architecture of WSNs and summarize state of the art in MAC and routing protocols for these networks.

2.2 Evolution of Wireless Sensor Networks

The early sensor networks were developed for military purpose during the Cold War, the Sound Surveillance System (SOSUS), a system of acoustic sensors (hydrophones), which was deployed on the ocean bottom at strategic locations to detect and track quiet Soviet submarines **[5]**. Modern research on sensor networks started around 1980s at the Defense Advanced Research Projects Agency (DARPA), the Distributed Sensor Networks (DSN) program was launched with the TCP/IP protocol invented for the ARPAnet (predecessor of the Internet) **[5]**. Since the end of 20^{th} century, MEMs, digital electronics, wireless communications, and other new IT technologies have been pushing the development of wireless sensor networks. At first few prestigious universities, i.e., MIT, UCLA, and Berkeley were involved in research of WSNs. Though the number of institutions and companies involved in research of WSNs expanded, there are still many open research issues waiting for resolutions such as the hardware design of the tiny sensors.

The sensor nodes are usually deployed in a sensor field randomly. Each of these nodes has capabilities to collect the data according to the applications (temperature, humidity, pressure, etc.) and route the data to the sink for further processing. Data is relayed to the sink through multi-hop wireless communications, and the user of the task manager can process and remotely control the system via the Internet or satellite. The basic structure of a sensor network is shown in Figure 1 [3].

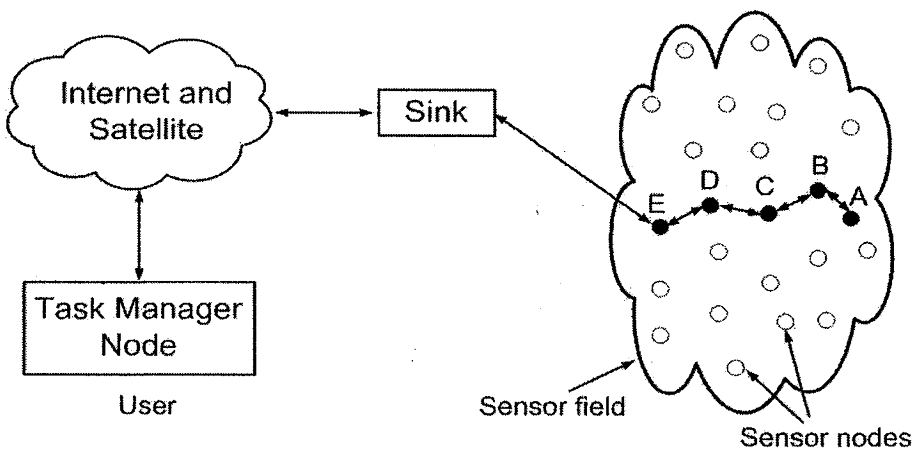


Figure 1: Sensor nodes scattered in a sensor field

There are four types of methods that nodes use to sense the environment and send the information to the sink.

- Continuous: a sensor continuously sends the information to a sink at a fixed frequency.
- Event-driven: a sensor sends information to a sink only when a pre-set event happens.

- Observer-initiated: if the observers find something abnormal, they will poll the sensor nodes to send information back to the control center.
- Hybrid: this case includes all the cases mentioned above.

A sensor node consists of four components as shown in Figure 2 [3]: a sensing unit, a processing unit, a power unit and a transceiver. It may also have other components such as location finding system, mobilizer, and power generation unit.

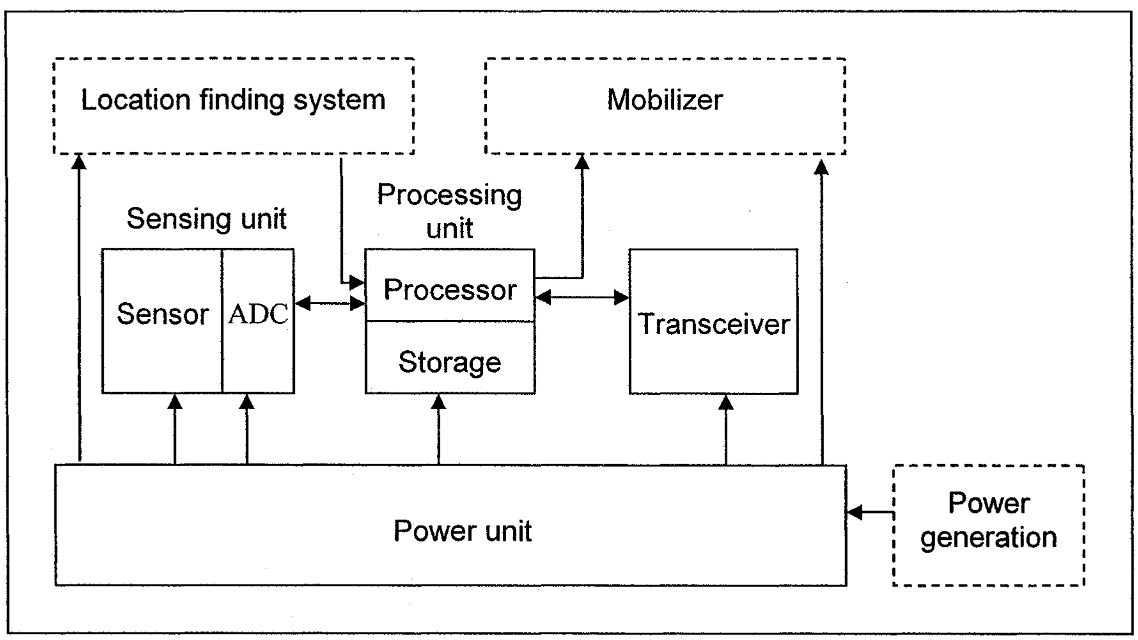


Figure 2: The components of a sensor node

Sensing units usually have two subunits, a sensor and an ADC. ADC converts the analog signals generated by the sensors following an observation to the digital signals which will be forwarded to the processors. The processing unit, which integrates small storage to store the information from ADC and transceiver, processes the information received from ADC and transceiver and enable the nodes to carry out their sensing tasks. The transceiver interconnects a node to the network, performs transmission and reception of the signals. An important component is the power unit, which supplies power to all of the subunits. Location finding system usually supports the techniques which require high location accuracy. Some sensor nodes have to move to adjust assignment tasks, so a mobilizer is a necessary component.

2.3 Most Recent Research Contributions to Wireless Sensor Networks

Presently, there are a number of research projects that have been undertaken at various educational institutions. All of these projects have been sponsored by the Defence Advanced Research Projects Agency of United States (DARPA).

Next, we describe the most important three of these projects.

(1) Massachusetts Institute of Technology (MIT):

MIT has proposed two protocols in the network layer. One of them is Low-Energy Adaptive Clustering Hierarchy (LEACH), which is a clustering-based protocol that minimizes energy dissipation in wireless sensor networks **[6]**. The other is Sensor Protocols for Information via Negotiation (SPIN) **[7]**, which sends data to sensor nodes only if they are interested, thus it avoids the energy dissipation by classical flooding.

(2) University of California-Los Angeles (UCLA)

Research at UCLA is mainly concerned with embedded systems and Wireless Integrated Network Sensors (WINS) architecture [8], which provides distributed Internet access to sensors and controls processors embedded in equipment, facilities, etc.

(3) University of California at Berkeley (UC-Berkeley)

UC-Berkeley's research has mainly two objectives: one is hardware, and the other is lab platform. The objective of Smart Dust [9] is the minimization of the hardware such that the sensing, computing and communication modules are integrated into a single chip. They have developed a series of hardware for sensor nodes and an embedded operating system, TinyOS, to simulate wireless sensor networks in the laboratory.

In Table 1, we present a list of some of the current research projects and their web addresses.

Project name	Research area	HTTP location
SensoNet **[10]**	Transport, network, data link, and physical layers. Power control, mobility, and task management planes.	http://www.ece.gatech.edu/research/labs/bwn/
WINS **[8]**	Distributed network and Internet access to sensors, controls, and processors.	http://www.janet.ucla.edu/WINS/
SPIN **[7]**	Data dissemination protocols.	http://nms.lcs.mit.edu/projects/leach
SPINS **[11]**	Security protocol.	http://paris.cs.berkeley.edu/~perrig/projects.html
SINA **[12]**	Information networking architecture.	http://www.eecis.udel.edu/~cshen/
μAMPS **[13]**	Framework for implementing adaptive energy-aware distributed microsensors.	http://www-mtl.mit.edu/research/icsystems/uamps/
LEACH**[6]**	Cluster formation protocol.	http://nms.lcs.mit.edu/projects/leach
Smart Dust **[9]**	Laser communication from a cubic millimeter. Mote delivery. Submicrowatt electronics. Power sources. Macro Motes (COTS Dust).	http://robotics.eecs.berkeley.edu/~pister/SmartDust/
SCADDS **[14]**	Scalable coordination architectures for deeply distributed and dynamic systems.	http://www.isi.edu/scadds/
PicoRadio **[15]**	Develop a "system-on-chip" implementation of a PicoNode.	http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/ PicoNode.htm
PACMAN **[16]**	Mathematical framework that incorporates key features of computing nodes and networking elements.	http://www.cs.pdx.edu/~singh/pacman.html

Dynamic Sensor Networks	Routing and power aware sensor management. Network services API.	http://www.east.isi.edu/DIV10/dsn/
Aware Home	Requisite technologies to create a home environment that can both perceive and assist its occupants.	http://www.cc.gatech.edu/fce/ahri
COUGAR Device Database Project	Distributed query processing.	http://www.cs.cornell.edu/database/cougar/index.htm
DataSpace	Distributed query processing.	http://www.cs.rutgers.edu/dataman/

Table 1: Current research projects

2.4 Wireless Sensor Network Protocol Architecture

Although WSN protocol architecture follows the OSI reference model, it has its own characteristics. The protocol stack of sensor networks consists of five layers: physical layer, data link layer, network layer, transport layer, and application layer. The following paragraphs present in some details this protocol stack.

- The Physical Layer

The physical layer is responsible for frequency selection, carrier detection, modulation and data encryption. Presently, the 915 MHz industry, scientific, and medical (ISM) band has been widely suggested for use by sensor networks. The choice of a good modulation scheme is critical for reliable communication in wireless sensor networks. Therefore, an energy efficient modulation method needs to be developed.

- The Data Link Layer

The data link layer is responsible for multiplexing data streams, data frame detection, and medium access which ensures reliable point-to-point and point-to-multipoint connection and error control. Medium access control (MAC) is the main function of this layer.

- The Network Layer

The network layer in a wireless sensor network is responsible for establishing a route from the resource node to the sink. In order to select the best route among a large number of paths, we have to take into consideration power efficiency and data-centric.

- The Transport Layer

This layer is especially needed when the system is to be accessed through the Internet or other external networks. TCP with its window mechanism is suitable for the wireless sensor network environment.

- The Application Layer

Many application areas for sensor networks are defined and proposed; the main protocols for this layer are the Management Protocol, Task Assignment and Data Advertisement Protocol, Sensor Query and Data Dissemination Protocol. Management Protocol makes the hardware and software of the lower layers transparent to the application layer, and it can turn the nodes on or off, or move the sensor nodes, etc. Task Assignment and Data Advertisement protocol makes the user to send its interest to a subset of the sensor network to complete specific tasks. Another approach is that the sensor nodes advertise the data to the users according to the users' interests. Sensor Query and Data Dissemination Protocol provides the user with the interface to respond to the queries and incoming replies.

2.5 MAC Protocol for Wireless Sensor Networks

In this section and the next one, we will describe the MAC protocols and routing protocols. Many researchers have been exploring new MAC and routing protocols that will minimize the energy dissipation in wireless sensor networks.

Traditional MAC protocols are not suitable for wireless sensor networks. In order to illustrate their limitations, we will take a closer look at the MAC protocols of other wireless networks.

In a ***cellular system***, the base stations form a wired backbone. A mobile node routes data to the nearest base station only by a single hop, and the goal of the MAC protocol is to provide high quality of service (QoS). The power consumption is not important because base stations have enough power supply to ensure uninterrupted work. In addition, the mobile node, our mobile phone, can be recharged or the battery can be changed when it dies or has low energy level. Such an access scheme is impractical for sensor networks because power efficiency directly influences the network lifetime.

Another system, ***Bluetooth or mobile ad hoc network (MANET),*** is close to sensor networks. This network is a wireless network that doesn't have base stations in the network. MANET uses TDMA as a MAC protocol because there are at most eight nodes in one piconet. Moreover, the primary goal of the MANET is high QoS. Although the nodes have portable battery equipped devices, they can be replaced or recharged by the user.

In contrast to these two schemes, a sensor network can consist of a large number of nodes. Hence, the power consumption is the first factor that needs to be taken into consideration when designing the MAC protocol. However, both fixed allocation (TDMA/FDMA/CDMA) and random access versions of MAC protocols have been proposed which are described below.

2.5.1 Scheduling based MAC Protocols

Self-Organizing Medium Access Control for Sensor Networks (SMACS) and the Eavesdrop-And-Register (EAR) Algorithm The SMACS protocol **[18]** achieves a network establishment, and the EAR algorithm enables a seamless connection of mobile nodes in a sensor network. In the SMACS protocol, the neighbour discovery and channel assignment phases are combined so that the nodes can hear all their neighbour nodes in the establishment, and then they can form a connected network by themselves. After establishment of a network, the EAR protocol attempts to keep continuous service to the mobile nodes under both mobile and stationary conditions.

SMACS allows a node to turn off its radio to conserve energy during idle periods. Each node maintains its own time slot schedule with all of its neighbours, which is called a superframe. Time slot assignment is only decided by the two nodes on a link, based on their available time randomly. It is possible that nodes will collide in the randomly chosen slots. Although the superframe looks like a TDMA frame, it does not prevent collisions between interfering nodes at all. To reduce the possibility of collisions, SMACS protocol can assign each link to operate on a different frequency band chosen at random from a large pool of channels. This protocol supports low-energy operation, but a disadvantage of it is the relatively low utilization of available bandwidth. A sub-channel is dedicated for each pair of nodes, but is only used for a small fraction of time, and it cannot be re-used by other neighbouring nodes.

Low-Energy Adaptive Clustering Hierarchy (LEACH) proposed by Heinzelman et al. [6] is an example of utilizing TDMA and clustering-based protocols in WSNs. Hierarchical network topology is adopted in LEACH protocol. Nodes are organized into many clusters, and TDMA has been used within each cluster by LEACH. The position of cluster head is rotated among nodes within a cluster depending on their remaining energy levels. Nodes in the cluster only talk to their cluster head, which then talks to the base station over a long-range radio. LEACH is an example of hybrid TDMA and CDMA. Frequency-hopping CDMA is adopted to handle inter-cluster communications and interference. However, TDMA-based protocol is used to handle intra-cluster communications between the cluster head (master) and its member nodes (slaves). The channel is divided into time slots for transmission, and the master node uses polling to decide which slave has the right to transmit. Only the communications between the master and one or more slaves is possible. The maximum number of active nodes within a cluster is limited to eight, an example of limited scalability. Larger networks can be constructed as in piconets, similar to Bluetooth, where one node bridges two piconets. The bridge node can temporarily leave one piconet and join another, or operate two radios.

The disadvantage of this protocol is that all member nodes in clusters are always listening to the channel for waiting the transmission from the cluster head even if the nodes are in idle state. Due to information exchange with the cluster-head, there is more overhead than that of peer-to-peer communication topology.

2.5.2 Contention-Based MAC Protocols

In contention-based MAC protocols a common channel is shared by all nodes and it is allocated on demand, unlike to the scheduled access that partitions the channel into a number of sub-channels for allocation to nodes permanently. A contention mechanism allows a node to access the channel at any moment.

Contention-based protocols have several advantages compared to scheduled protocols. First, they can be more flexible to adapt to changes in topology because bandwidth is assigned on demand. Second, they have no requirement to form clusters, and the peer-to-peer communication topology is directly supported. Finally, contention-based protocols do not require precise time synchronizations as in TDMA protocols. While, the major disadvantage of a contention protocol is its inefficient usage of energy. Because it is highly probable that a node will collide with others when they access the shared channel, much energy of the system will be wasted for retransmission of information. Overcoming this disadvantage is required if contention-based protocols are to be applied to long-lived sensor networks.

Carrier Sense Multiple Access (CSMA) based protocol is an important contention based protocol. The main idea of CSMA is listening to the shared channel and detecting if the medium is busy before transmitting. There are several variants of CSMA, including non-persistent, 1-persistent, and p-persistent CSMA. In non-persistent CSMA, if a node detects an idle medium, it transmits immediately. If the medium is busy, it waits a random amount of time and starts carrier sensing again. In 1-persistent CSMA, a node transmits if the medium is idle. Otherwise it continues to listen until the medium becomes idle, and then transmits immediately. In p-persistent CSMA, a node transmits with probability p if the medium is idle, and with probability $(1 - p)$ back-offs and restarts carrier sensing.

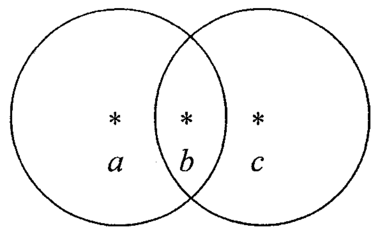


Figure 3: Hidden terminal problem

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In a multi-hop wireless network, however, CSMA alone is not sufficient due to the hidden terminal problem which is illustrated in Figure 3 on a two-hop network with three nodes. Suppose nodes *a, b* and *c* can only hear from their immediate neighbours. As a result, when node *a* is transmitting to *b*, node *c* is not aware that the channel is busy, and its carrier sense still indicates that the channel is idle. Therefore, *c* starts to transmit, *b* will receive collided packets from *a* and *c*. CSMA/CA protocol was developed to address the hidden terminal problem, and is adopted as the wireless LAN standard, IEEE 802.11 **[19]**. The basic mechanism in CSMA/CA is to establish a brief handshake between a sender and a receiver before the sender transmits data. The sender sends a short Request-to-Send (RTS) packet to the receiver. After receiving the RTS, the receiver replies the sender with a Clear-to-Send (CTS) packet, which informs its neighbours that there will be a transmission from a sender. The sender starts sending data after it receives the CTS packet. The purpose of RTS-CTS handshake is to make an announcement to the neighbours of both the sender and the receiver. In the example of Figure 3, although node *c* cannot hear the RTS from *a*, it can hear the CTS from *b*. If a node hears an RTS or CTS destined to other nodes, it should back-off without sending its own packet. CSMA/CA does not completely eliminate the hidden terminal problem, but now the collisions are mainly on RTS packets. Since the RTS packet is very short, the cost of collisions is greatly reduced.

Based on CSMA/CA, Karn and Bharghavan *et al* proposed MACA **[20]** and MACAW **[21]**, which add some additional information to packets such as duration field in both RTS and CTS packets indicating the amount of data to be transmitted, and an acknowledgment (ACK) packet after data packets. These measures can make other nodes know how long they should back-off and offer error free transmission. Thus, the transmission between a sender and a receiver follows the sequence of RTS-CTS-DATA-ACK.

S-MAC Protocol in Wireless Sensor Networks **[22]**, suggested by the researchers at the University of California, Los Angeles, is an improved contention-based MAC protocol. It uses several novel techniques to reduce power consumption and support self-configuration: nodes periodically sleep, avoid collisions, and apply message passing.

The first technique in S-MAC protocol is sleep and wakeup cycle that allows nodes to be in sleep status most of the time. Each cycle begins with a listen period for nodes to send data, and a sleep period follows if the nodes have no data to send or receive.

During the sleep period, a node turns off its radio, and sets a timer for waking up later on. All nodes are free to choose their own listen and sleep schedules. They share their schedule with their neighbours to let them know when they wakeup and sleep. Then, nodes could schedule transmission during the listen period of destination nodes. S-MAC requires looser synchronization because this protocol has a relatively long listen period compared to the short period of time in waking up. Each node maintains a table that stores the schedules of all its known neighbours by exchanging the scheduling information so that all neighbouring nodes can talk to each other even if they have different schedules.

Next technique is the collision avoidance mechanism. The collision avoidance mechanism in S-MAC is similar to that in IEEE 802.11. Contention only happens at a receiver's listen interval. Unicast packets follow the sequence of RTS-CTS-DATA-ACK between the sender and the receiver, while broadcast packets are sent without RTS and CTS procedure by sender. S-MAC puts a duration field in each packet, which indicates the time needed in the current transmission. If a neighbouring node receives any packet from the sender or the receiver, it knows how long it needs to keep silent. In this case, S-MAC puts the node into sleep state for this amount of time, avoiding energy waste on overhearing. Ideally the node goes to sleep after receiving a short RTS or CTS packet destined to other nodes, and it avoids overhearing subsequent data and ACK packets.

The last technique in S-MAC protocol is message passing. An important feature of wireless sensor networks is in-network data processing, since data aggregation or other techniques can greatly reduces energy consumption by largely reducing the amount of data to be transmitted. In traditional MAC layer, if we fragment the long message into many independent small packets, we have to pay the penalty of large control overhead because the RTS and CTS packets are used in contention for each small packet. However, in message passing of S-MAC protocol, only one RTS and one CTS are used to reserve the medium for the time needed to transmit all the fragments of a message. Each fragment is separately acknowledged, and sender will retransmit the fragment immediately if ACKs are missed. Besides RTS and CTS, each fragment or ACK also has the duration field to indicate the time needed for transmitting all the remaining data fragments and ACK packets, allowing nodes that wake up in the middle of the transmission to return to sleep. This is unlike 802.11's fragmentation mode where each fragment only indicates the presence of an additional fragment, not all of them.

2.5.3 Brief Introduction of MAC Protocol of IEEE 802.15.4

Although the research on wireless sensor networks has been intensifying, there is no accepted commercial standard. However, some researchers considered adopting the IEEE 802.15.4-2003 Low Rate Wireless Personal Area Network (LR-WPAN) **[17]** standard for wireless sensor networks.

Next, we briefly describe the MAC protocol of IEEE 802.15.4 which adopts a contention-based CSMA/CA protocol.

There are two kinds of devices in WPANs, one Reduced-Function Device (RFD), and the other Full-Function Device (FFD). A FFD can communicate with other FFDs or RFDs, but a RFD only communicates with a FFD. Each PAN has exactly one coordinator, a Full-Function Device only, which is configured to provide synchronization services through the transmission of beacons. The MAC protocol of IEEE 802.15.4 can work on both beacon-enabled and non-beacon-enabled modes. In the non-beacon-enabled mode, each device communicating with other devices adopts unslotted CSMA/CA protocol. Most of the new features of IEEE 802.15.4 standard are in the beacon-enabled mode. Therefore, we have to observe the frame structure of beacon-enabled mode of IEEE 802.15.4 standard.

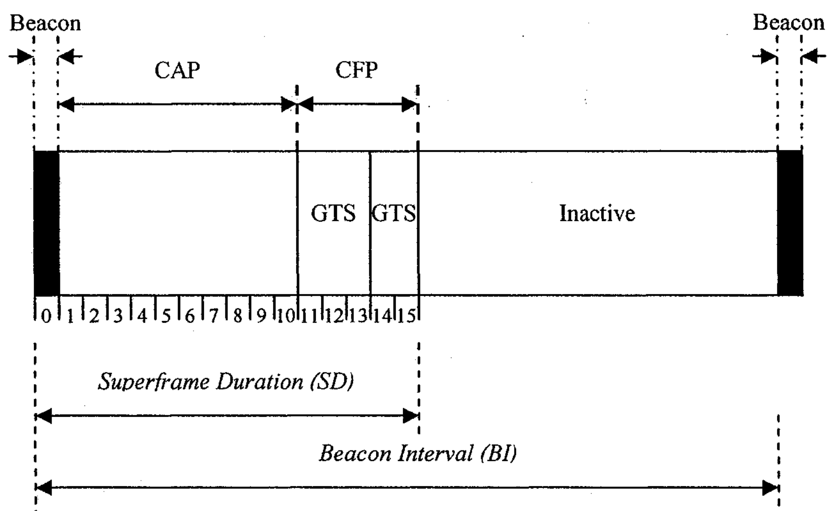


Figure 4: An example of the IEEE 802.15.4 superframe structure

In beacon-enabled mode, IEEE 802.15.4 uses superframe structure shown in **Figure 4 [17]**. A superframe is bounded by the transmission of a beacon frame periodically sent by PAN coordinator. A superframe has both active and inactive portions. Devices can communicate with each other during active portion, and enter a low power status during inactive portion.

The active portion of the superframe can be divided into 16 time slots and consists of three parts: a beacon, a Contention Access Period (CAP), and a Contention Free Period (CFP). CFPs are only presented if guaranteed time slots (GTS) are allocated by the PAN coordinator to some of the devices. The CFP starts on a slot immediately following the CAP. Each GTS consists of some integer multiple of CFP slots and up to 7 GTSs are allowed in CFP.

When a device communicates with others and transmits data, if it has been allocated a GTS by coordinator, it sends its own data in CFP; otherwise it sends data using a slotted CSMA/CA mechanism to access the channel.

2.6 Routing Protocols for Wireless Sensor Networks

For similar reasons, traditional routing protocols are impractical for wireless sensor networks. First, WSNs have no global addressing scheme; therefore, classic IP-based routing protocol cannot be applied to sensor networks. Second, generated data traffic has significant redundancy in the network because multiple sensors may generate the same data within the vicinity. Last, sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage. Several new routing protocols have been proposed for WSNs including their performance modeling **[23],[24].** The routing protocols can be divided into three classes: data-centric, hierarchical and location-based.

2.6.1 Data Centric Protocol

Flooding and Gossiping: Flooding and gossiping routing protocols are two classical mechanisms to relay data in sensor networks. In flooding, each sensor node receives the packet and then broadcasts it to all of its neighbours. Each node repeats this process until the packet reaches to the destination or the maximum number of hops for the packet can be reached. Although flooding is very easy to disseminate data, it has some drawbacks such as *implosion,* and *overlap*. *Implosion* means a large amount of duplicated messages are sent by the same node. *Overlap* is caused by different nodes sensing the same area and sending similar data to the same neighbour. Therefore, much energy is wasted for transmission of a large amount of duplicated messages. The other approach is gossiping which is a slightly enhanced version of flooding. After receiving data, the node relays it to a randomly selected neighbour, which picks another random neighbour to forward the packet to and so on. Gossiping solves the implosion by selecting a random node to send the packet rather than broadcasting. However, this causes delays in propagation of data through the network.

Sensor Protocols for Information via Negotiation (SPIN) **[7]**, which solves the problem of a large amount of duplicated information when flooding or gossiping is used in the network. The idea of SPIN is to name the data using a descriptor or meta-data. Before a node wants to send data to its neighbors, the sensor node broadcasts an ADV message to its neighbor, which is meta-data containing a descriptor of the DATA message. The neighbor nodes compare the descriptor of the DATA message to information in memory. If the neighbor is interested in the data, it sends back a request (REQ) message for the DATA, otherwise the neighbor ignores the DATA. SPIN's meta-data negotiation solves the classic problems of redundant information passing and overlapping of sensing areas. **Figure 5** summarizes the steps of the SPIN protocol.

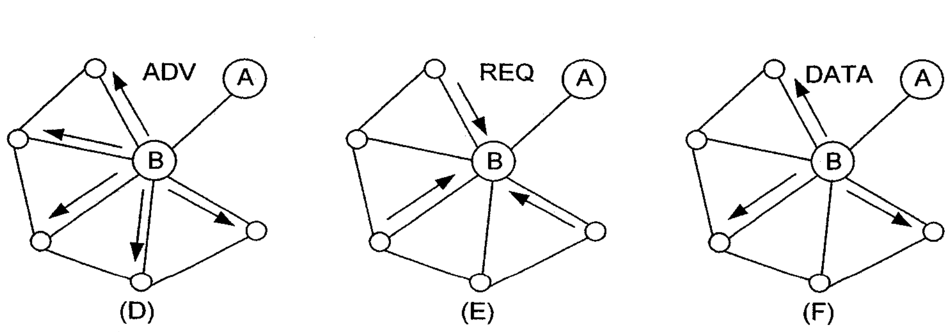


Figure 5: An example of SPIN protocol

In **Figure 5** (A), node A advertises meta-data to node B; (B) node B responds by sending a request to node A; (C) After receiving the request, node A sends data to node B; (D) node B sends advertisement to its neighbour; (E) interested nodes respond by sending their requests to node A; and (F) node B sends data to interested nodes.

However, SPIN's data advertisement mechanism cannot guarantee the delivery of data because the nodes that are interested in the data may be very far away from the source node. Therefore, reliable delivery of data packets over regular intervals is necessary.

Directed Diffusion The Directed Diffusion data dissemination is proposed in **[25]**. The main reason using such a scheme is to get rid of unnecessary operations of network layer routing in order to save energy. This is a task based protocol. The key feature in Direct Diffusion is the use of task descriptions. For example, we want to know the movement of four-legged animals in one region. We have to establish some attribute-values to describe this task such as the type of observed objects, four-legged animals in this example, time interval, the frequency of data sent back to sink, and the scope of observed region, etc. All the information is used to describe some tasks, and a task description is called *interest*.

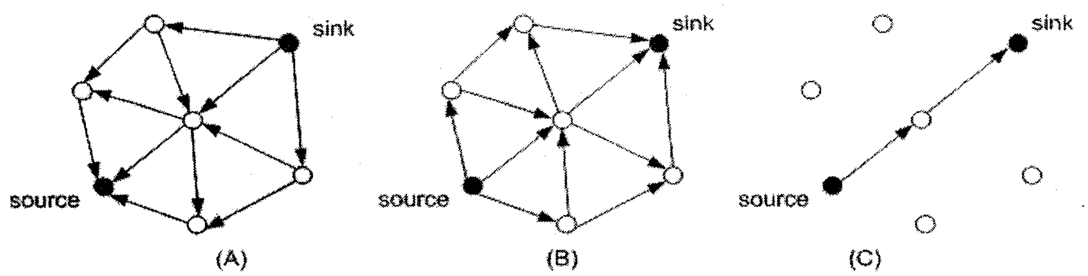


Figure 6: An example of directed diffusion protocol

The procedure of Directed Diffusion protocol is described as follows. The sink sends out the interest to its neighbours as shown in **Figure 6 (A)**. The interest entry contains a timestamp field and several gradient fields. As the interest is propagated throughout the sensor network, the gradients from the source back to the sink are set up as shown in **Figure 6 (B)**, and one of several paths is selected by reinforcement which is the rule to select the best path such as low energy consumption, or low delay. Finally, when the source has data for interest, or the sink has query of interests, the communication between sink and source can be implemented through the selected path with the best efficiency as shown in **Figure 6 (C)**.

2.6.2 Hierarchical Protocol

Similar to other communication networks, scalability is one of the major design attributes of sensor networks. In a flat structure of network, the communication with gateway or sink could produce very long latency delay, even congestion, because a large amount of data has to be processed in the gateway or sink. In addition, flat structure is not good to expand the network because the maximum number of hops for transmission increases in a wider area. In order to solve the problem of load, hierarchical-based protocols have been proposed. Hierarchical routing is mainly two-layer routing where one layer is used to select cluster-heads and the other layer is used for routing. A large amount of volume of data processing is completed in cluster-head nodes, so the protocol is good to expand the network.

Another advantage of hierarchical routing is energy efficient. In the architecture, higher energy nodes can be used to process and send the information, while low energy nodes can be used to perform the sensing in the proximity of the target. The position of cluster head could be rotated among nodes within a cluster depending on their remaining energy levels.

Low-Energy Adaptive Clustering Hierarchy (LEACH), is one of the clustering-based protocols that minimizes energy dissipation in wireless sensor networks. In LEACH, the cluster-head process data arriving from nodes that belong to the respective cluster, and sends an aggregated packet to the gateway or sink as explained before LEACH uses a TDMA/CDMA MAC protocol to reduce inter-cluster and intra-cluster collisions. This protocol has two stages: setup and steady. During setup phase, the system will select the cluster-head using a specific algorithm. New cluster-heads will advertise to all the nodes in the network that they are new. Once the sensor nodes receive the advertisement, they will determine which cluster-head they should belong in terms of the strength of advertisement signals. Last, the cluster-heads assign the timeslot to their underling to allow them communication with cluster-heads based on a TDMA protocol. During steady-phase, the cluster-heads can process the data before sending them to the sink or base station. After certain period of time, the steady-phase could change to the setup-phase again because some conditions have changed, for example, the power capacity of some cluster-heads may be very low. Therefore, the system enters another round of selecting cluster-heads.

2.6.3 Location-based protocols

There is no global address scheme in wireless sensor networks because of the characteristics of WSNs mentioned above. Therefore, we cannot locate the nodes like IP address in wireless ad hoc networks. Most of the routing protocols for sensor networks only use location information for sensor nodes. In most cases location information is needed in order to calculate the distance between two particular nodes so that energy consumption can be estimated. The location information can be utilized in routing data in an energy efficient way. Many energy aware routing protocols of wireless sensor networks based on the location information have been proposed.

MECN and SMECN: Minimum Energy Communication Network (MECN) **[26]** and Small Minimum Energy Communication Network (SMECN) **[27]**.

MECN protocol utilizes low power GPS module integrated to the sensor nodes to acquire location information, and to maintain minimum energy consumption in the network. The main idea of MECN is to find a sub-network, which will have less number of nodes and require less power for transmission between any two particular nodes.

SMECN protocol is an enhanced version of MECN protocol. In MECN, it is assumed that every node can transmit to every other node, which is not possible every time. In SMECN, the possible obstacles between any pair of nodes are considered. Meanwhile, the sub-network constructed by SMECN for minimum energy relaying is probably smaller than the one constructed in MECN if the broadcast region is circular around the broadcasting node for a given power setting.

This completes the survey of network architecture for WSN. In the next chapter, we will present a performance analysis of a MAC protocol for WSN.

CHAPTER 3:

MODELING OF SENSOR NETWORKS

3.1 Introduction

After review of wireless sensor networks, we know that conservation of power is critical for the long term operation of the network.

The energy efficiency requires that the sensor devices are not operated continuously, and it is suggested that sensor nodes have at least two modes of operation as active and sleep modes. In active state a node is fully operational while in the sleep mode the sensor does not take part in the network activities. In sleep mode, a sensor node will not consume energy and it may also be able to recharge its batteries. An important design problem is how to schedule the sleeping and active periods of the network nodes such that the connectivity of the network is preserved. We have to consider this scheduling under the MAC protocol of the system. As discussed in the previous chapter, MAC protocols for WSN may be TDMA or contention based. As indicated, contention protocols are wasteful of bandwidth. As a result, we have assumed a TDMA media access protocol for our study. In a TDMA system, the frame will have enough timeslots to accommodate all the nodes in the network. However, this is not practical in high density sensor networks, and therefore slot reuse has been proposed to take advantage of limited transmission capabilities of the nodes as well as their alternation between active and sleep periods **[29][30]**. Thus, the nodes within transmission range of each other needs to be assigned different slots. The proposed MAC protocol consists of a fully distributed and self-organizing time-division multiple access (TDMA) scheme. Several approaches have been proposed to manage access to the TDMA slots **[31]**.

The objective of this work is to present a performance analysis of a wireless sensor network with the TDMA media access protocol. It is assumed that the packet arrivals to each node are according to a Poisson process and each node serves to the arrivals according to the *FCFS* service discipline. The packets are routed to a sink node according to a routing matrix through intermediate nodes. The sleep periods may consists of several exponentially distributed stages and the arrival processes of the nodes are disabled during the sleep periods. The sleeping nodes also relinquish their slots in the TDMA frame. We model the sensor networks with open network of queues with unreliable nodes. The sleeping periods of sensor nodes are modeled as breakdowns of nodes in a Jackson network, which allows us to make use of the results from **[32]**. However, the application of those results poses two problems, the sensor networks have finite state space compared to Jackson networks and that wake up of a node may be blocked due to unavailability of slots in the TDMA frame. Following the resolution of these problems, we determine the joint distribution of the queue lengths in a sensor network. Then, the probability distribution of the number of active nodes and blocking probability of node activation are derived. Then, we determine the mean packet delay and average sleeping period of a node, the network throughput. The model also captures reduction of traffic load due to elimination of duplicated information among the collected data.

3.2 Modeling of the System

In this part, we will establish the system model for the performance analysis of WSN. First, we describe Jackson type of open network of queues, and then introduce node breakdowns. Following that, we model WSN as a Jackson type of network. Finally, we derive performance measures of WSNs.

3.2.1 Jackson Networks

We begin with the description of Jackson type of open network of queues with single servers **[33]**. The Jackson network is defined as follows.

A Jackson network model consists of a network of service stations (nodes) $\bar{J} = \{1, 2, \ldots, j, \ldots, J\}$, and the *j'th* node has a single server with *FCFS* service discipline. The external customers arrive at node *j* according to a Poisson process with arrival rate of λ_j. Both internal and external customers arriving at node *j* request an exponentially distributed service time with mean $1/\mu_j$, and all the service times are assumed to be independent of each other.

After receiving service at node *i*, a customer selects the next node *j* with transition probability $r(i, j)$, and then enters node *j* to receive service; or a customer selects to leave the network immediately with probability $r(i, 0)$ (we use "0" to denote the departures from the network, so $\sum_{j=0}^{J} r(i, j) = 1$).

The traffic equation for node j is given by,

$$e_j = \lambda_j + \sum_{i=1}^{J} e_i r(i,j), \ j = 1,....,J \tag{1}$$

If we denote $\mathbf{e} = [e_1, e_2, ..., e_J]$, $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, ..., \lambda_J]$ and $\mathbf{R} = \begin{bmatrix} r_{11} & & r_{1J} \\ & \ddots & \\ r_{J1} & & r_{JJ} \end{bmatrix}$, then equation (1) can be written in the following matrix form,

$$\mathbf{e} = \boldsymbol{\lambda} + \mathbf{eR} \tag{2}$$

the simultaneous solution of the above system of equations determines the total arrival rate of each node e_j. The Jackson's theorem shows that the steady state joint probability distribution function of queue length is given by the *product form*,

$$\pi(n_1, ..., n_J) = K(J)^{-1} \prod_{j=1}^{J} \left(\frac{e_j}{\mu_j} \right)^{n_j} \tag{3}$$

with normalization constant $K(J)$.

3.2.2 Modeling of Jackson's Network with Unreliable Nodes

In this section, we introduce a model of networks with unreliable nodes. We specifically consider Jackson networks with node breakdowns and repairs studied in **[32]**.

We describe the node breakdown and repair processes which are Markovian. The nodes may be in one of two states, up or down states. A node in the down state is under repair and all the arrivals to that node are blocked. The external arrivals are set to zero and the internal arrivals destined to the blocked node remain at their present location and receive a repeat service. Following, the repeat service they choose a new destination according to the routing matrix. Thus routing probabilities are modified as follows,

$$\tilde{r}(i,j) = \begin{cases} r(i,j), & i,j \in \overline{I}_U^*, i \neq j \\ r(i,i) + \sum_{k \in \overline{I}_D} r(i,k), & i \in, \overline{I}_U^*, i = j \\ otherwise & \end{cases} \quad \textbf{(4)}$$

where $\overline{I}_U$ and $\overline{I}_D$ denote the set of the nodes in the up and down statuses respectively and $\overline{I}_U^* = \{\overline{I}_U \cup 0\}$ also includes the zero node. We consider the special case that breakdown and repair of the nodes are independent of each other and it depends only to the local load. We let $a_i(n_i)$ and $b_i(n_i)$ denote the breakdown and repair rate of node i with local load n_i when it is in the up and down statuses respectively. Then, the breakdown and repair intensities of the network at state $\boldsymbol{n}$ are given by,

$$A\ (n_i : i \in \overline{I}_U) = \prod_{i \in \overline{I}_U} a_i(n_i) \quad \text{and} \quad B\ (n_i : i \in \overline{I}_D) = \prod_{i \in \overline{I}_D} b_i(n_i) \quad \textbf{(5)}$$

Next, we assume that the nodes may breakdown only if they are empty and they have constant breakdown and repair rates with α and β respectively. Thus the amount of time that will elapse before an empty node may breakdown and repair time of a down node are exponentially distributed with parameters α and β respectively. Next letting

$|\bar{I}_U|$ and $|\bar{I}_D|$ denote the number of nodes in sets $\bar{I}_U$ and $\bar{I}_D$ respectively, then the network breakdown and repair intensities are given by,

$$A\ (n_i : i \in \bar{I}_U) = \alpha_i^{|\bar{I}_U|} \prod_{i \in \bar{I}_U} \delta_{0n_i} \quad \text{and} \quad B\ (n_i : i \in \bar{I}_D) = \beta_i^{|\bar{I}_D|} \prod_{i \in \bar{I}_D} \delta_{0n_i} \tag{6}$$

where $\delta_{0n_i} = \begin{cases} 1 & n_i = 0 \\ 0 & otherwise \end{cases}$

We let $\pi(\boldsymbol{n})$ denote the joint probability distribution of queue length vector, then it is given by,

$$\pi(\boldsymbol{n}) = \pi(n_1, \ldots, n_J) = C^{-1} \prod_{j=1}^{J} \rho_j^{n_j} \tag{7}$$

$$\pi(\bar{I}_D, \boldsymbol{n}) = \pi(\bar{I}_D; n_1, \ldots, n_J) = C^{-1} \frac{A(n_i : i \in \bar{I}_D)}{B(n_i : i \in \bar{I}_D)} \prod_{j=1}^{J} \rho_j^{n_j}, \quad \forall \bar{I}_D \neq \varnothing \tag{8}$$

with $\rho_j = e_j / \mu_j$, and the normalization constant C is given by,

$$C = \sum_{\boldsymbol{n} \in E} \left[\prod_{j=1}^{J} \rho_j^{n_j} \left(1 + \sum_{\substack{\bar{I}_D \subset J \\ \bar{I}_D \neq \phi}} \frac{A(n_i : i \in \bar{I}_D)}{B(n_i : i \in \bar{I}_D)} \right) \right] \tag{9}$$

$$= \sum_{\boldsymbol{n} \in E} \left[\prod_{j=1}^{J} \rho_j^{n_j} \left(1 + \sum_{\substack{\bar{I}_D \subset J \\ \bar{I}_D \neq \phi}} \left(\frac{\alpha_i}{\beta_i} \right)^{|\bar{I}_D|} \prod_{i \in \bar{I}_D} \delta_{0n_i} \right) \right]$$

$$= \prod_{j=1}^{J} \left(\frac{1}{1-\rho_j} + \frac{\alpha_j}{\beta_j} \right) \qquad \textbf{(10)}$$

where E is the total state space of the joint queue length vector of the Jackson network, and the equation (10) means that the contribution of each node to the normalization constant is in one of the two forms: $1/(1-\rho_j)$ in the up state, and α_j/β_j in the down state.

3.2.3 Performance Analysis of Wireless Sensor Networks

3.2.3.1 The Modeling of Wireless Sensor Networks

Now, we describe modeling of sensor networks with Jackson networks with breakdown and repairs introduced in the above.

Each node of the sensor network may be in either active or sleeping mode and the state of the network is determined by the combined states of all the nodes. We may model active and sleep states with up and down statuses of a Jackson node respectively. The packet transmission corresponds to customer service at a node. While packet lengths do not change during transfer of packets from node to node in the network, service times in a Jackson network are independent identically distributed. As usual, this approximation is justified by Kleinrock's independence assumption **[34]**.

From the above explanation, we may model a sensor network with a Jackson type of network with unreliable nodes. However, a sensor network may only have a truncated state space of a Jackson network. We will assume circular transmission ranges with sharp boundaries, which means there is no signal and interference received outside of transmission ranges; each node lies within the transmission range of at least one other node. We let $\overline{M}_j$ denote the set of the nodes within the transmission range of node j including itself. Thus the transmission of a node will interfere with the transmissions of all the nodes within its transmission range. This problem may be solved by assigning nodes within each others' transmission ranges to different time slots. Therefore, the number of active nodes within the transmission range of a node cannot exceed the number of time slots in a TDMA frame. Let us define $r_{\max}$ to denote the number of slots in a frame. Thus, we should have $\left|\overline{M}_{Uj}\right| \le r_{\max}$ for all nodes $j \in \overline{J}$, and this condition will be referred to as the feasibility criteria. As a result, only those states of Jackson's networks that satisfy the feasibility criteria will be admissible in a sensor network, these states will be referred to as feasible states. We should be able to classify each state as feasible or not and the feasibility has to be path independent. In a sensor network, the order that the nodes become active may determine whether a state is feasible or not. We will assume that if there is any order of node activation that allows a state to be feasible, then this state will be classified as feasible. In practice, this may be achieved through the reassignment of the slots to the nodes in the TDMA frame, however if this is not possible, then our results will provide an upper-bound to the performance of the target sensor network.

Thus from the above discussion a sensor network will have a truncated state space of the corresponding Jackson network and all the feasible states will be reachable from each other. Then, the joint distribution of queue length vector of a sensor network may be obtained from the corresponding distribution of Jackson's networks through normalization **[[35], pp.26]**. We let $\{\Omega = \Omega_U \cup \Omega_D\}$ denote the truncated network state space with subspaces Ω_U corresponding to the union of network states where all nodes are in the up status and Ω_D corresponding to the network states that have at least one node in the down status. Also letting $\overline{\pi}(\boldsymbol{n})$, $\overline{\pi}(\overline{I}_D, \boldsymbol{n})$ denote the sensor network queue length distribution, then,

$$\begin{aligned} \overline{\pi}(\boldsymbol{n}) &= G^{-1}\ \pi(\boldsymbol{n}), & \forall\ \boldsymbol{n} \in \Omega_U \\ \overline{\pi}(\overline{I}_D, \boldsymbol{n}) &= G^{-1}\ \pi(\overline{I}_D, \boldsymbol{n}), & \forall\ \boldsymbol{n} \in \Omega_D \end{aligned} \qquad \textbf{(11)}$$

where, $G = G_1 + G_2$ with $\begin{cases} G_1 = \sum_{\boldsymbol{n}\in\Omega_U} \pi(\boldsymbol{n}) = \sum_{\boldsymbol{n}\in\Omega_U} \prod_{j=1}^{J} \frac{1}{1-\rho_j} \\ G_2 = \sum_{\boldsymbol{n}\in\Omega_D} \pi(\overline{I}_D, \boldsymbol{n}) = \sum_{\boldsymbol{n}\in\Omega_D} \prod_{j=1}^{J} W_j \end{cases}$,

with $W_j = \begin{cases} \frac{1}{1-\rho_j} & \text{, if node } j \text{ is up} \\ \frac{\alpha_j}{\beta_j} & \text{, if node } j \text{ is down} \end{cases}$,

and also where $\pi(\boldsymbol{n})$, $\pi(\overline{I}_D, \boldsymbol{n})$ are given by equations (7),(8).

As described in Chapter 2, the data collected by neighbouring nodes may be identical, and duplicated information may be transmitted to the sink. As we have seen, some routing protocols assume that sensor nodes have capacity to detect duplicated data received from its neighbours, and not to forward them. Our sensor network model may capture this by allowing departures from the network at intermediate nodes. Thus, when a packet arrives to node j from i, node j will check its content, and if duplicate, it will drop it. In the model under study, this will be taken into consideration by letting departures from network after receiving service at a node j.

3.2.3.2 DERIVATION OF PERFORMANCE MEASURES

Next, from the joint queue length distribution, we will derive several performance measures.

- **Distribution of the number of active nodes**

First, we will determine the probability distribution of the number of active nodes, $q(k)$,

$$q(k) = \begin{cases} G_1 & \text{if } (k = J) \cap (\bar{I}_D = \varnothing) \\ \sum_{n \in \Omega} \bar{\pi}(\bar{I}_D, \boldsymbol{n}) & \text{if } (k = J - |\bar{I}_D|) \cap (\bar{I}_D \neq \varnothing) \end{cases} \tag{12}$$

where, k is the number of active nodes in system. Then, the average number of active nodes in the system is given by,

$$\bar{k} = \sum_{k=0}^{J} k * q(k) \tag{13}$$

- **Probability that a node is active**

Next, we determine probability that a node is active. Let us define φ_j , $\bar{\varphi}$ as follows,

$$\varphi_j = \text{Prob(node } j \text{ is active)}$$

$$\bar{\varphi} = \text{Prob(a node is active)}$$

Then,

$$\bar{\varphi} = \frac{1}{J}\sum_{j=1}^{J} \varphi_j = \frac{\bar{k}}{J} \tag{14}$$

- **Wake up blocking probability**

Third, we derive the probability that a sleeping node's activation will be blocked. Since down periods are exponentially distributed, an awakening node will see the system at equilibrium like a random observer. Let us define $\bar{\boldsymbol{M}}_{Uj}$ as the set of active nodes within the transmission range of node j at a given network state $\boldsymbol{n}$. Clearly, if node j wakes up in a network state that $\bar{\boldsymbol{M}}_{Uj}$ equals to $r_{\max}$, then it will be blocked, therefore defining,

$$P_j = \text{Prob}\left[\text{activation of node } j \text{ will be blocked}\right]$$

$$P_j = \frac{1}{\sum_{\forall\{j\in\bar{I}_D\}} \bar{\pi}(\bar{I}_D,\boldsymbol{n})} \sum_{\substack{n \\ \forall\{j\in\bar{I}_D\cap|\bar{M}_{Uj}|=r_{\max}\}}} \bar{\pi}(\bar{I}_D,\boldsymbol{n}) \qquad \textbf{(15)}$$

where the summation in the denominator corresponds to waking up probability of node j.

- **Marginal queue length distribution**

Next, we determine the marginal distribution of the queue length of node j, which is denoted to $p(n_j)$. This may be obtained from equations **(11)** by summing up with respect to the other random variables,

$$p(n_j) = \begin{cases} \bar{\phi}_j \dfrac{\alpha_j}{\beta_j} & \text{node } j \text{ is in sleep, } n_j = \mathbf{0} \\ \bar{\phi}'_j \rho_j^{n_j} & \text{node } j \text{ is active, } n_j \geq \mathbf{0} \end{cases} \qquad \textbf{(16)}$$

where, $\bar{\phi}_j = \frac{1}{G} \sum_{\{n\in\Omega_D \cap j\in\bar{I}_D\}} \prod_{i\neq j} W_i$, and $\bar{\phi}'_j = \frac{1}{G}\left\{ \sum_{\{n\in\Omega_D \cap j\notin\bar{I}_D\}} \prod_{\{i\neq j\}} W_i + \sum_{n\in\Omega_u} \prod_{\substack{i=1 \\ i\neq j}}^{J} \frac{1}{1-\rho_i} \right\}$, with

$$W_i = \begin{cases} \dfrac{1}{1-\rho_i} & \text{, node } i \text{ is up} \\ \dfrac{\alpha_i}{\beta_i} & \text{, node } i \text{ is down} \end{cases}$$

- **Mean queue length and packet delay at a node**

The average queue length at node j is given by,

$$\bar{n}_j = \sum_{n_j=0}^{\infty} n_j p(n_j) \tag{17}$$

where, $p(n_j)$ is from equation (16). We may express $\bar{n}_j$ as follows,

$$\bar{n}_j = \sum_{n_j=0} n_j p(n_j) + \sum_{n_j=1}^{\infty} n_j p(n_j)$$

$$= \sum_{n_j=1}^{\infty} n_j p(n_j) = \sum_{n_j=1}^{\infty} n_j \bar{\phi}'_j \rho_j^{n_j}$$

$$= \bar{\phi}'_j \sum_{n_j=1}^{\infty} n_j \rho_j^{n_j} = \frac{\bar{\phi}'_j}{1-\rho_j} \sum_{n_j=0}^{\infty} n_j (1-\rho_j) \rho_j^{n_j}$$

Finally, the average queue length of node j is given by,

$$\bar{n}_j = \frac{\bar{\phi}'_j \rho_j}{(1-\rho_j)^2} \tag{18}$$

From the application of Little's result, the mean packet delay is given by,

$$\bar{d} = \frac{1}{\lambda \bar{\varphi}} \sum_{j=1}^{J} \bar{n}_j \tag{19}$$

where λ is the total external arrival rate of the packets, $\lambda = \sum_{j=1}^{J} \lambda_j$, and $\lambda \bar{\varphi}$ gives the total rate of traffic admission to the network with $\bar{\varphi}$ as defined in (14).

- **Distribution of time that a node is down**

Next, we will determine the distribution of the time that a node spends in the sleep state, time interval between two consecutive active states of a node. The sleep period of each node may consist of a random number of exponentially distributed down periods. As explained above the wake up of a node may be blocked if all the slots of the TDMA system within its transmission range are occupied, then, the node is forced to take an additional down period and repeat this process at the next wake up time. Assuming that the blocking of the consecutive wake ups are independent of each other,

$\alpha_j(r)$ = Prob [node j will experience r consecutive down periods]

$= (1-P_j)\, P_j^{r-1} \qquad r = 1, 2, 3\ldots.$

where P_j is given by (15).

Letting θ_j denote the sleep duration of node j and x_i i'th down period, then,

$$\theta_j = \sum_{j=1}^{\alpha_j} x_i$$

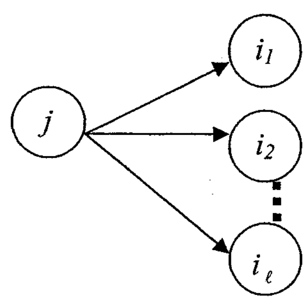
Since down periods are exponentially distributed with parameter β, the mean sleeping period of node j is given by,

$$\overline{\theta}_j = \overline{\alpha}_j \overline{x}_i = \frac{1}{\beta(1-P_j)} \qquad \textbf{(20)}$$

- **the average throughput of the network**

Next, we determine the departure rate of packets from the network due to duplication of information. The removal of duplicated information will result in reduction of traffic load. As explained before, this may be taken into account by allowing departure of packets form the network at the intermediate nodes. We let $r(j,0)$ denote the probability that a packet will leave the network after service at node j.

We assume that a node will drop only from the information generated by its immediate neighbours. Let us assume that node j forwards the traffic to nodes $\bar{i} = \{i_1, i_2, \cdots, i_\ell\}$ as shown in the following figure. The rate of total traffic, e_j, being



forwarded to the set of nodes $\bar{i}$ from node j, but only λ_j of this traffic is generated by node. Each of the receiving nodes will drop a packet directly generated by node j with probability σ. Therefore, the rate of flow reduction by nodes $\bar{i}$ will be $\lambda_j\sigma$. Thus the departure rate of traffic from the network following service at node j is

$$r(j,0) = \frac{\lambda_j \sigma}{e_j}$$

Following this adjustment, the new routing probabilities will be given by

$$r'(j,k) = [1 - r(j,0)]\, r(j,k)$$

Finally, defining S as the average throughput of the network, we have,

$$S = \lambda \bar{\varphi}\ \mathbf{(1\text{-}\sigma)} = \frac{\lambda \bar{k}\,\mathbf{(1\text{-}\sigma)}}{J} \qquad \mathbf{(21)}$$

The above completes the derivation of performance measures for sensor networks.

CHAPTER 4:

NUMERICAL RESULTS

In this chapter, we present some numerical results regarding the analysis in the thesis. We consider as an example of a wireless sensor network with 16 nodes. We present performance measures for this network both with and without packet drop. We also discuss how these results may be used in the design of sensor networks.

4.1 Network Topology

Before continuing our study, we will repeat the main assumptions. The circular transmission boundary is sharp, which means we can not receive any signals and interference outside of transmission ranges. The other is that each node lies in the reception range of at least one other node; otherwise, there are no overlap between transmission ranges, so the information could not be transmitted to the sink.

In **Figure 7**, we present the topology of the 16-node network under study. As may be seen, there is also an additional sink node. We have shown only the coverage areas of the first three nodes in order to prevent crowding of the figure. **Table 2** gives the connectivity matrix of the network. An asterisk at the intersection of a row and a column shows that the corresponding nodes are within the coverage area of each other. Each row gives the coverage area of a node.

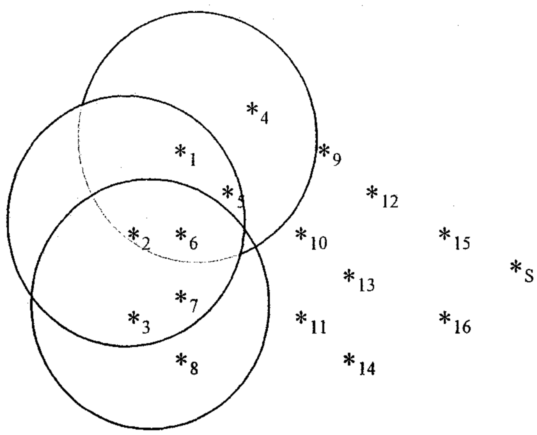


Figure 7: The topology of the 16-node wireless sensor network

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	*	*		*	*	*										
2	*	*	*		*	*	*									
3		*	*			*	*	*								
4	*			*	*				*							
5	*	*		*	*	*			*	*						
6	*	*	*		*	*	*			*	*					
7		*	*			*	*	*			*		*			
8			*				*	*			*					
9				*	*				*	*		*				
10					*	*			*	*			*		*	
11						*	*	*			*		*	*		
12									*			*	*		*	
13							*			*	*	*	*	*	*	*
14											*		*	*		*
15										*		*	*		*	
16													*	*		*

Table 2: The connectivity matrix of the 16-node wireless sensor network

The **Table 3** presents the routing matrix of the network. Each row corresponds to the routing probabilities of a node. Non-zero routing probabilities are shown by the letters, *u, v, w,* and *x* which have the values of 1/4, 1/3, 1/2, 1 respectively. Sink node, S, is within the transmission range of nodes 15 and 16 which forward all their traffic to it. In the numerical results, this is achieved by setting the departure probability from the network for these nodes to one. Thus following a service at nodes 15 or 16, the packets depart from the system. In the following numerical results, we assume that the traffic arrival rates to all of the nodes are equal except for sink node which is zero.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1		*u*		*u*	*u*	*u*										
2			*u*		*u*	*u*	*u*									
3						*v*	*v*	*v*								
4					*w*				*w*							
5						*v*			*v*	*v*						
6							*v*			*v*	*v*					
7								*v*			*v*		*v*			
8											*x*					
9										*w*		*w*				
10													*w*		*w*	
11													*w*	*w*		
12													*w*		*w*	
13														*v*	*v*	*v*
14																*x*
15																
16																

Table 3: The routing matrix of a 16-sensor network

4.2 Performance Measures for the Example Network without Packet Drop

In this section we present performance measures for the example network without dropping of packets in the intermediate nodes.

Figure 8 presents the average number of nodes in the active state as a function of the number of slots in a frame, r_{max}, with the ratio of sleep to wake up rate, α/β, and packet arrival rate, λ, as parameters from equation **(13)**. As the ratio decreases the nodes spend more time in active as opposed to sleep state. (As the λ increases, the more nodes are in active status.) As a result, it may be seen that for any given value of r_{max}, average number of nodes increases with the decrease of the parameter α/β.

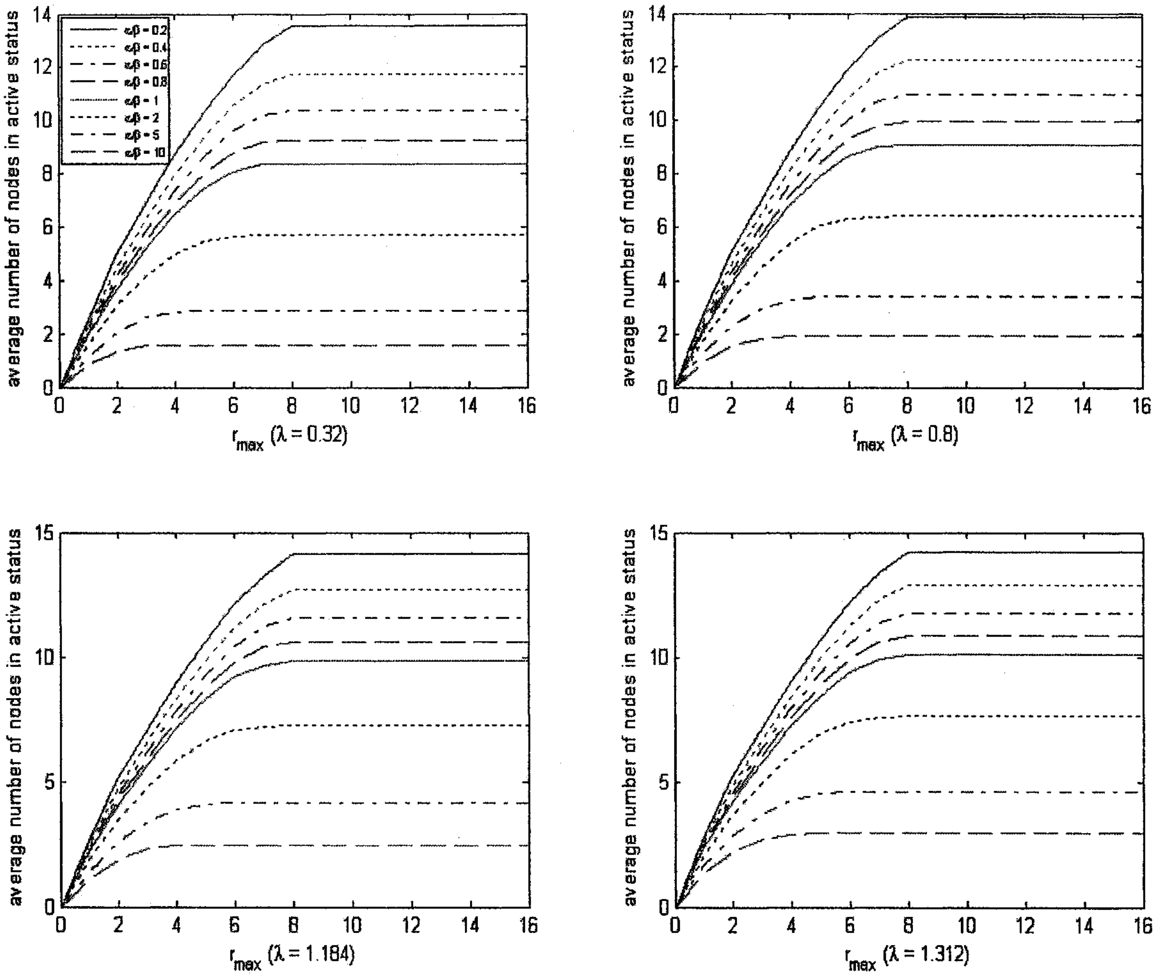


Figure 8: The average number of nodes in active state as a function of frame size in slots, r_{max}

Figure 9 shows blocking probability of wake up for selected nodes as a function of the frame size in slots, r_{max} from equation **(15)**. As expected blocking probability drops down as r_{max} increases.

Figure 10 shows average sleep period of selected nodes as a function of $r_{\max}$ for selected nodes from equation **(20)**. The average sleeping time of each node goes down as r_{max} increases. When the $r_{max} = 0$, which means all the nodes are sleeping, the average sleeping time of each node becomes infinite. As the r_{max} increases, the sleeping time goes down. When a node's wake up cannot be blocked, the sleeping time consists of an exponentially distributed period which has the mean $1/\beta$.

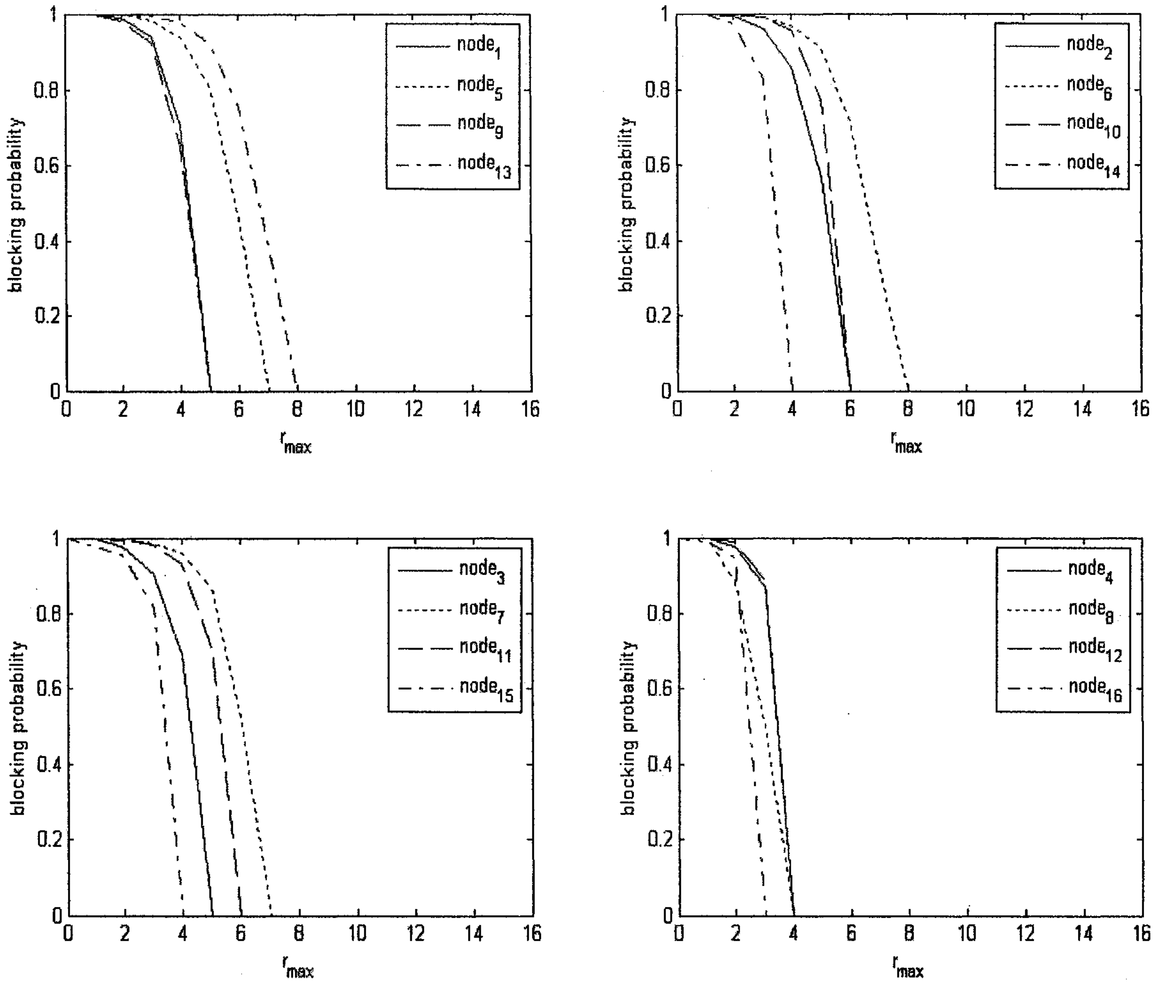


Figure 9: The blocking probability of wake up for selected nodes as a function of r_{max}

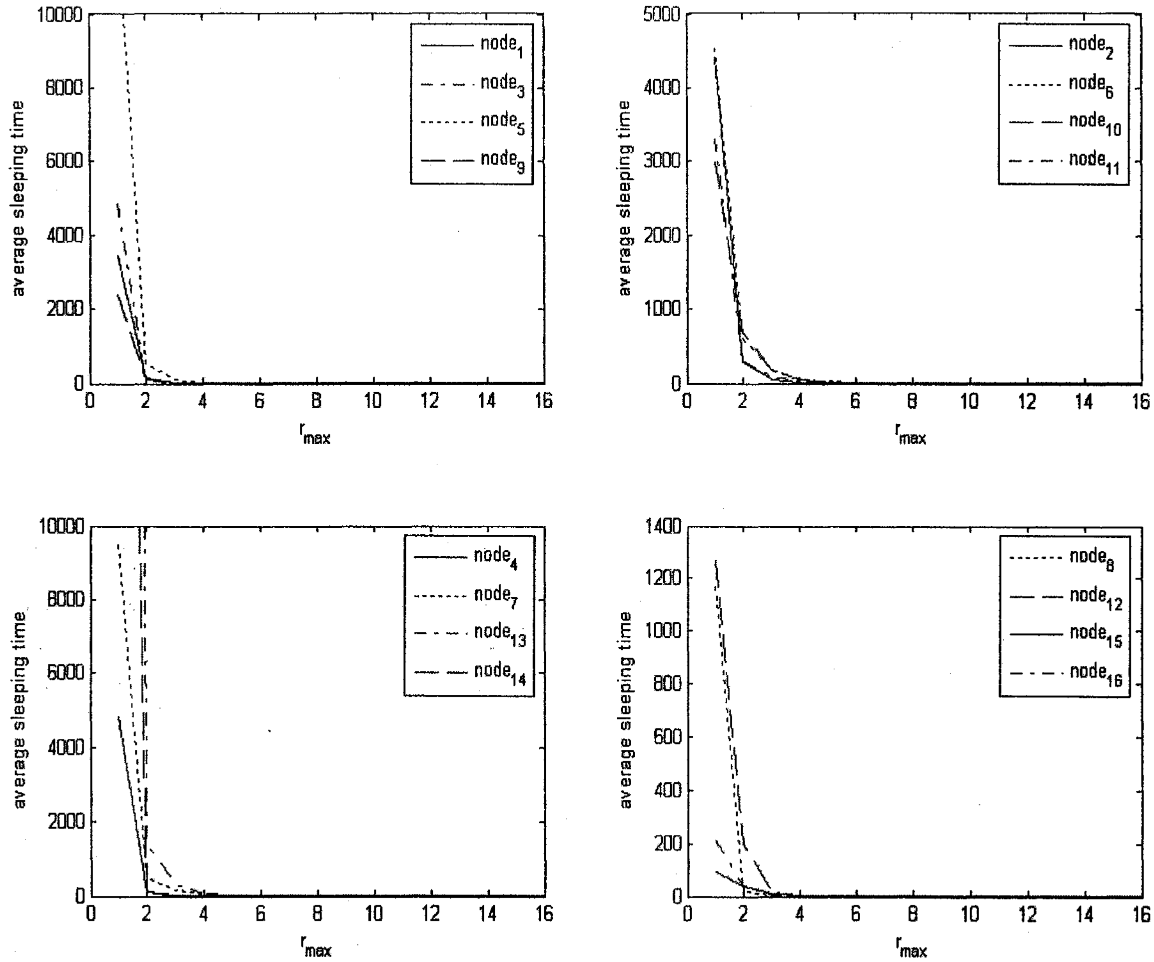


Figure 10: The average sleep period of selected nodes as a function of r_{max}

Figure 11 presents the average packet delay as a function of the total arrival rate λ for a given value of the sleep to wake up rate ratio with r_{max} as the parameter from equation **(19)**. As expected, the average delay drops with increasing r_{max}.

Figure 12 shows average delay as a function of the sleep to wake up ratio for a given value of the total arrival rate with r_{max} as a parameter from equation **(19)**. As may be seen, mean delay rises as α/β increases since again average number of nodes in the sleep status increases.

Figure 13 presents the average throughput of the system as a function of the number of slots in a frame, r_{max}, with total arrival rate λ as a parameter from equation **(21)** . It may be seen that average throughput in creases with r_{max} initially but then it becomes flat.

Figure 14 presents the average throughput of the system as a function of the total arrival rate λ, with r_{max} as a parameter from equation **(21)**. The average throughput increases slowly as the r_{max} increases for any fixed value of the total arrival rate. Initially, the throughput increases far more significantly, as the number of slots in a frame increases for any fixed value of arrival rate. As may be seen, throughput does not increase anymore after frame size reaches to eight.

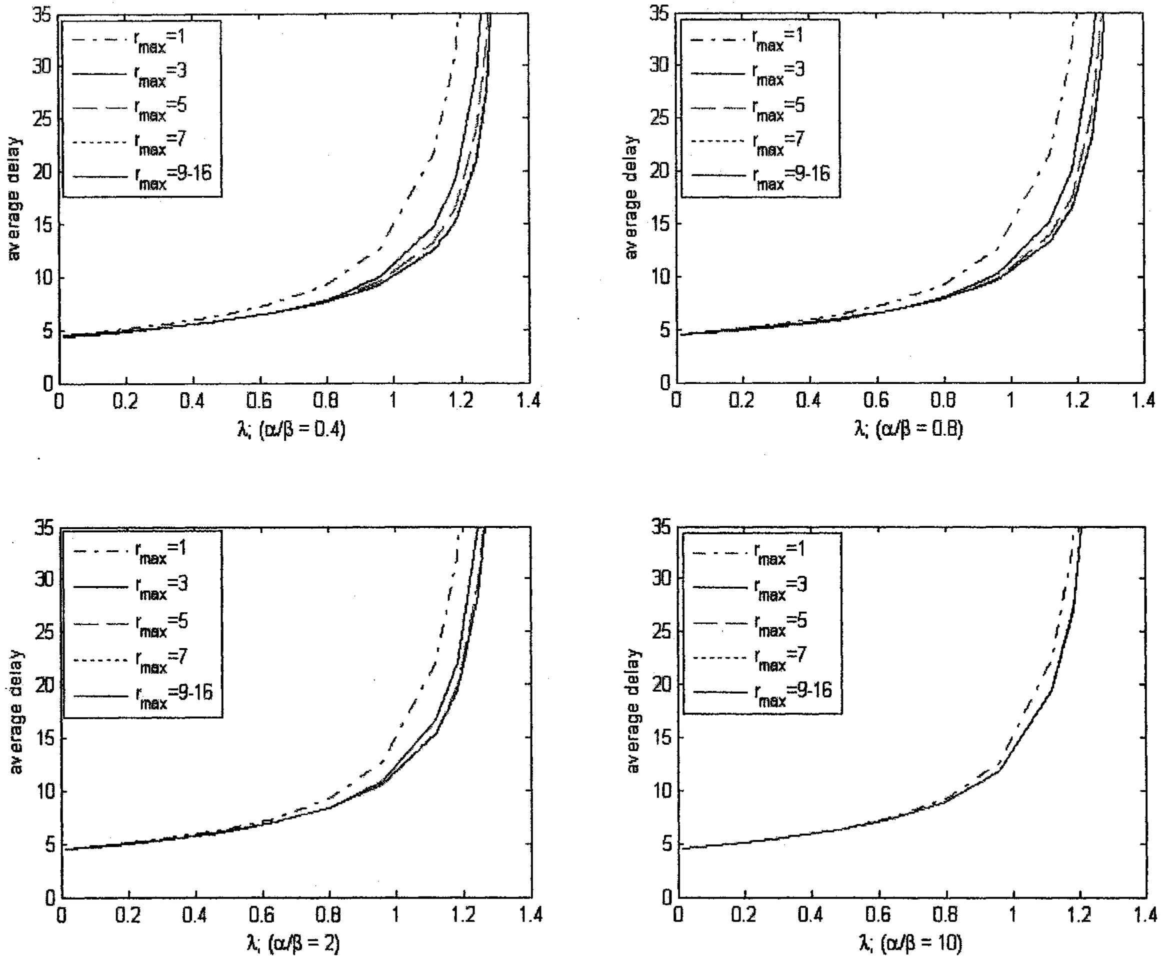


Figure 11: The average delay as a function of total arrival rate, λ, with r_{max} as a parameter

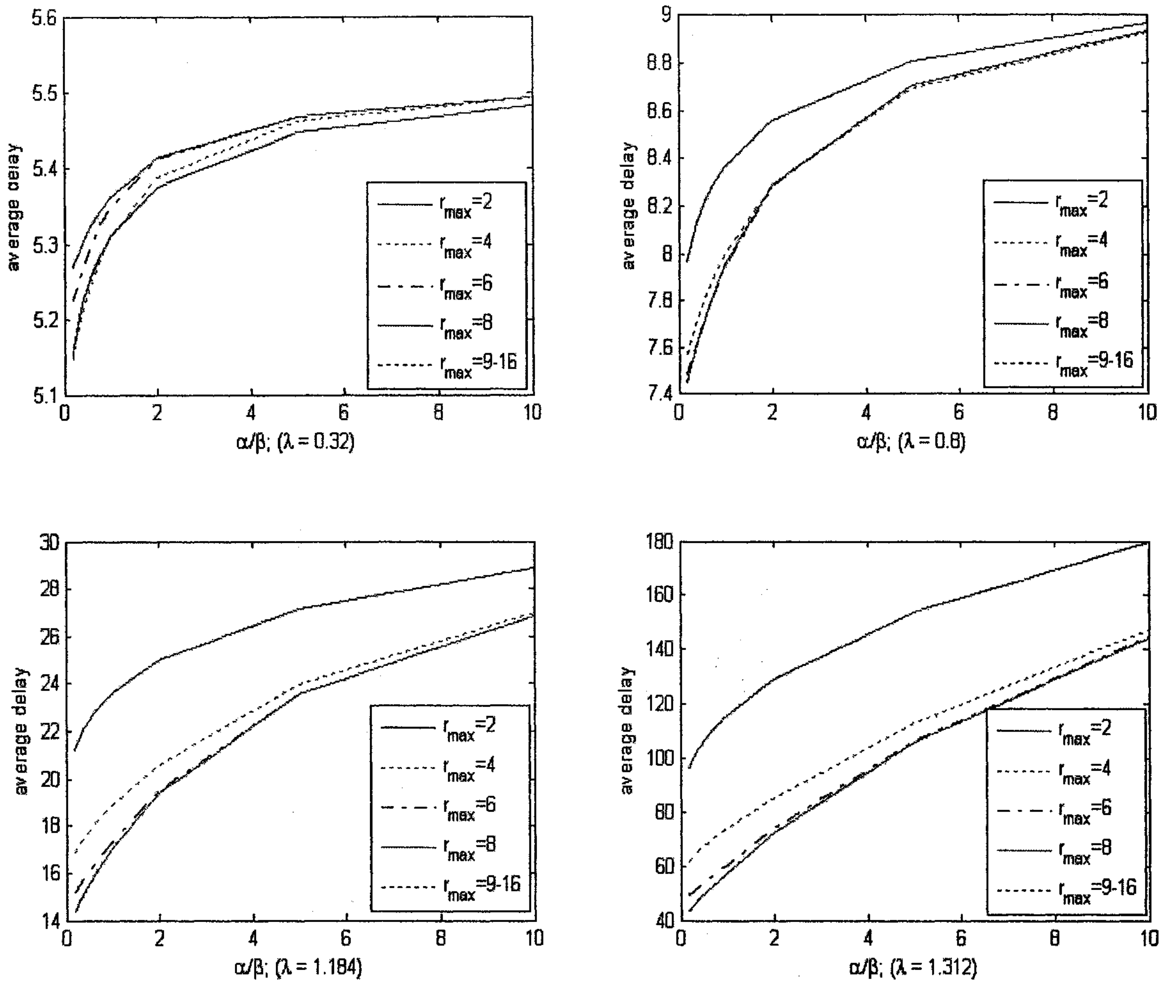


Figure 12: The average delay as a function of the sleep to wake up rate ratio α/β with r_{max}

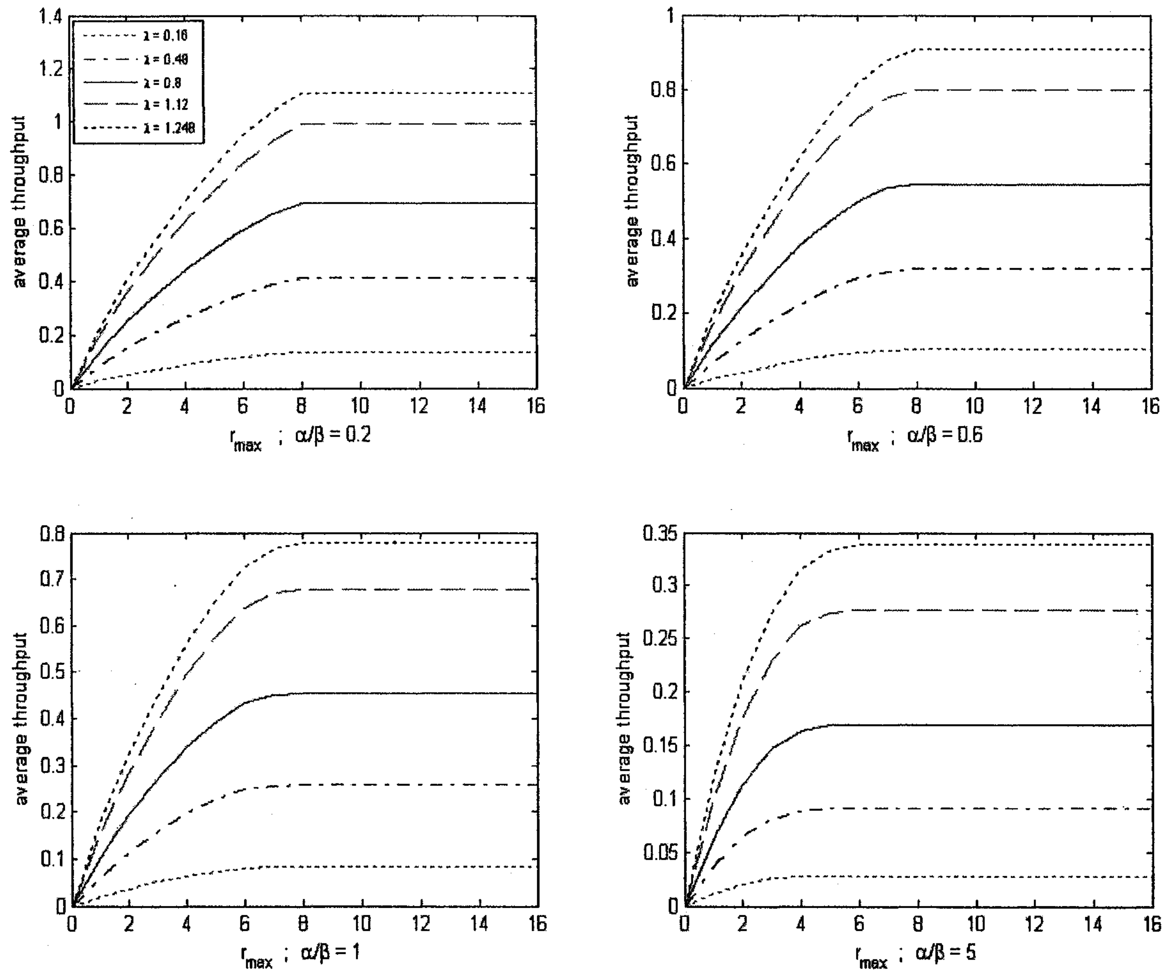


Figure 13: The average throughput as a function of r_{max} with total arrival rate as a parameter

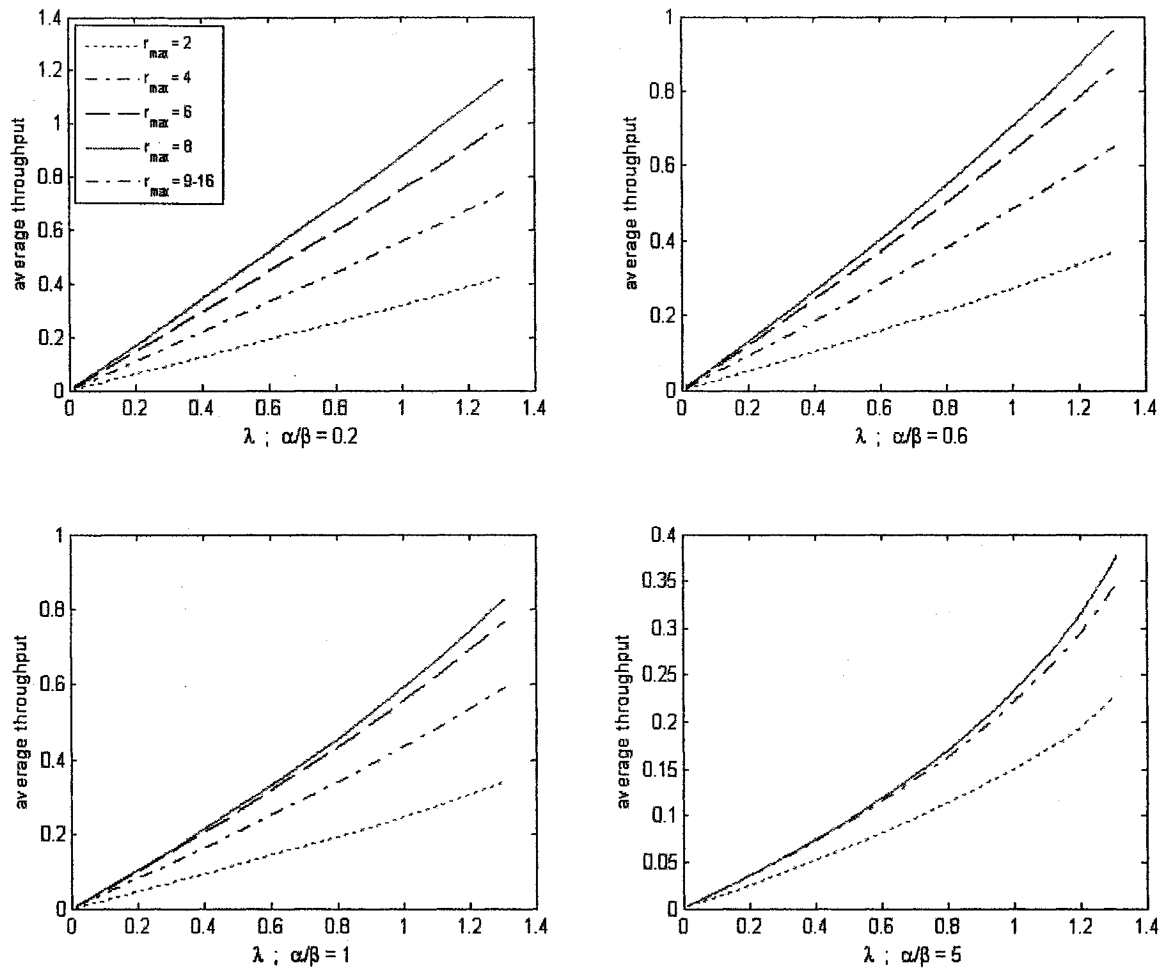


Figure 14: The average throughput as a function of the total arrival rate, λ, with r_{max} as a parameter

4.3 Performance Measures for the Example Network with Packet Drop

In this section, we present the numerical results for the same sensor network but with packet drop. The network topology and connectivity remain same, but routing matrix is changed. It is assumed that due to duplication in the collected date, the intermediate nodes may drop some of the received packets from their neighbours. This is captured by allowing departure from the network at intermediate nodes.

From **Figure 15 to Figure 21**, we present corresponding to **Figure 7 to Figure 14** for the network. Most figures are very similar to the ones without packet drop except for delay and throuhput figures. The comparison of curves in Figures 11, 12 with those in Figure 18,19 shows that mean delay decreases with the introduction of packet drop.

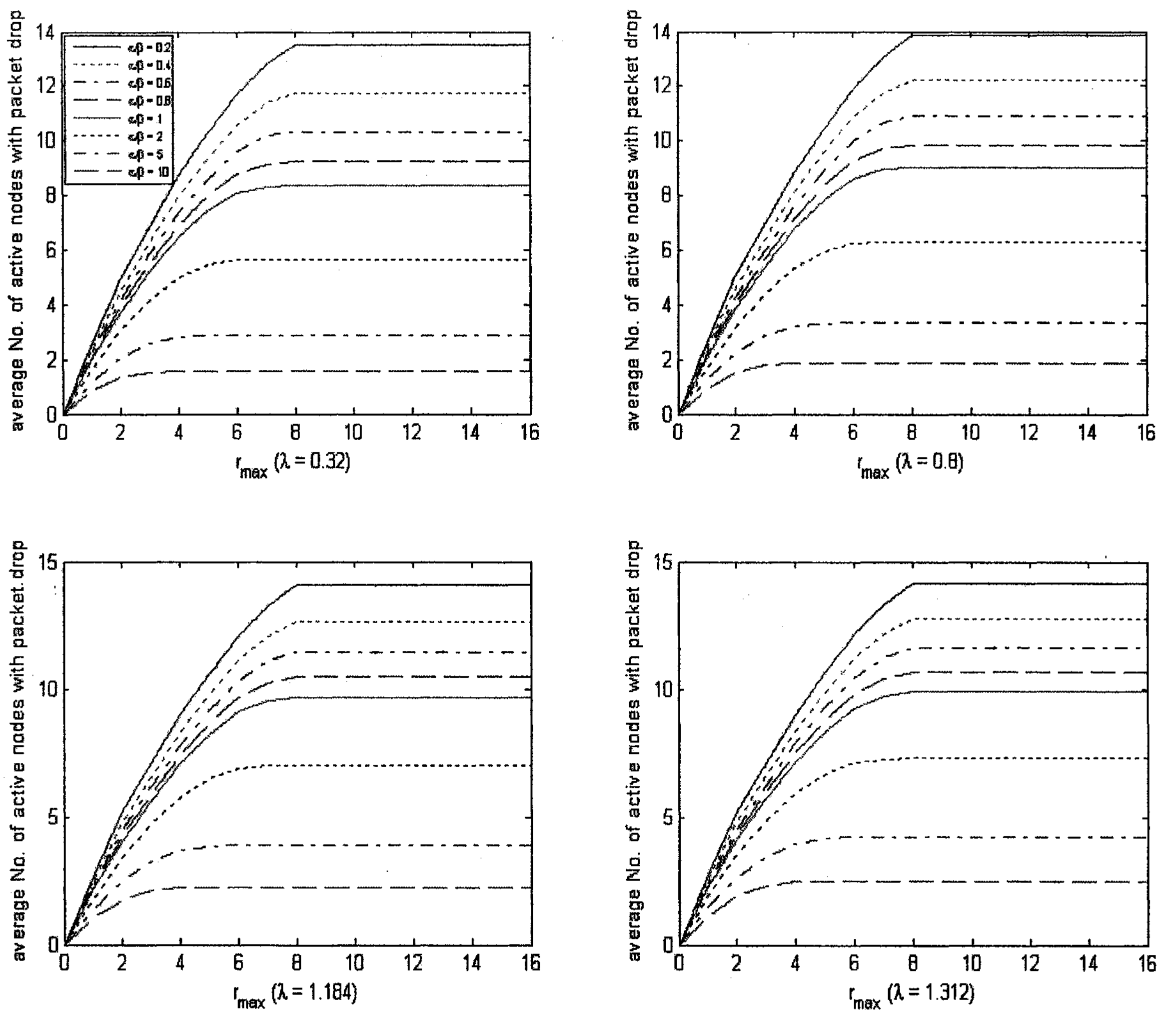


Figure 15: The average number of nodes in active state as a function of frame size in slots, r_{max} with packet drop

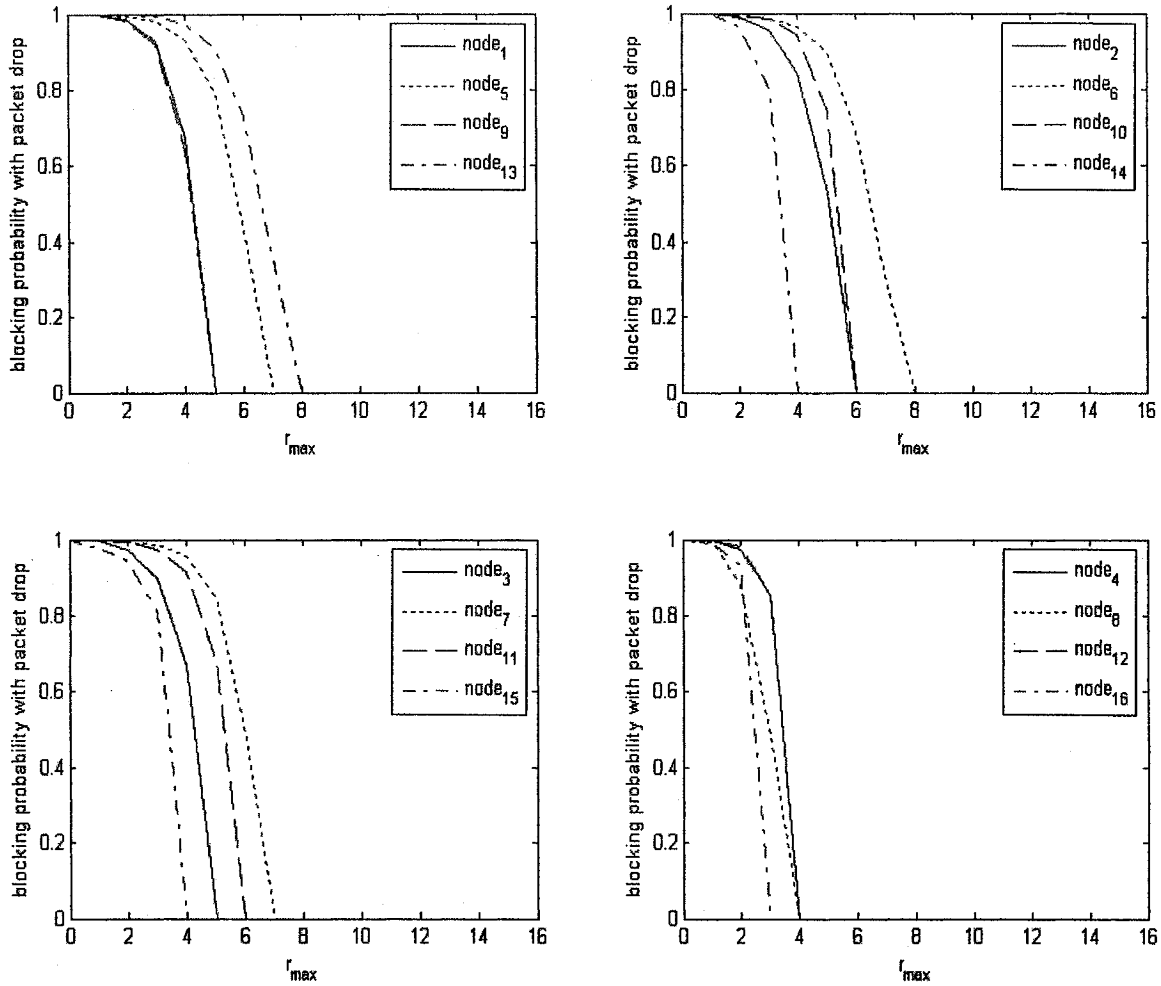


Figure 16: The blocking probability of wake up for the selected nodes as a function of r_{max} with packet drop

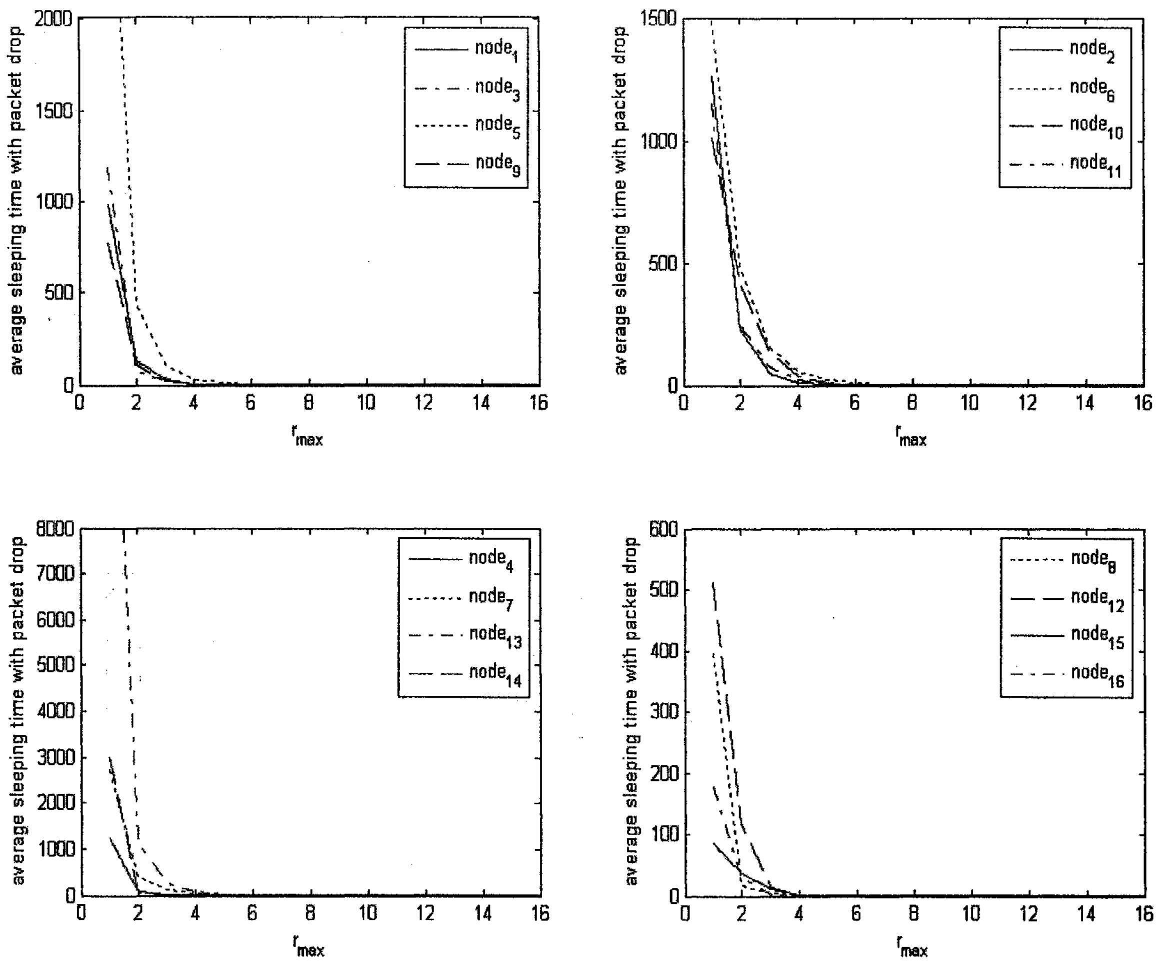


Figure 17: The average sleep period of selected nodes as a function of r_{max} with packet drop

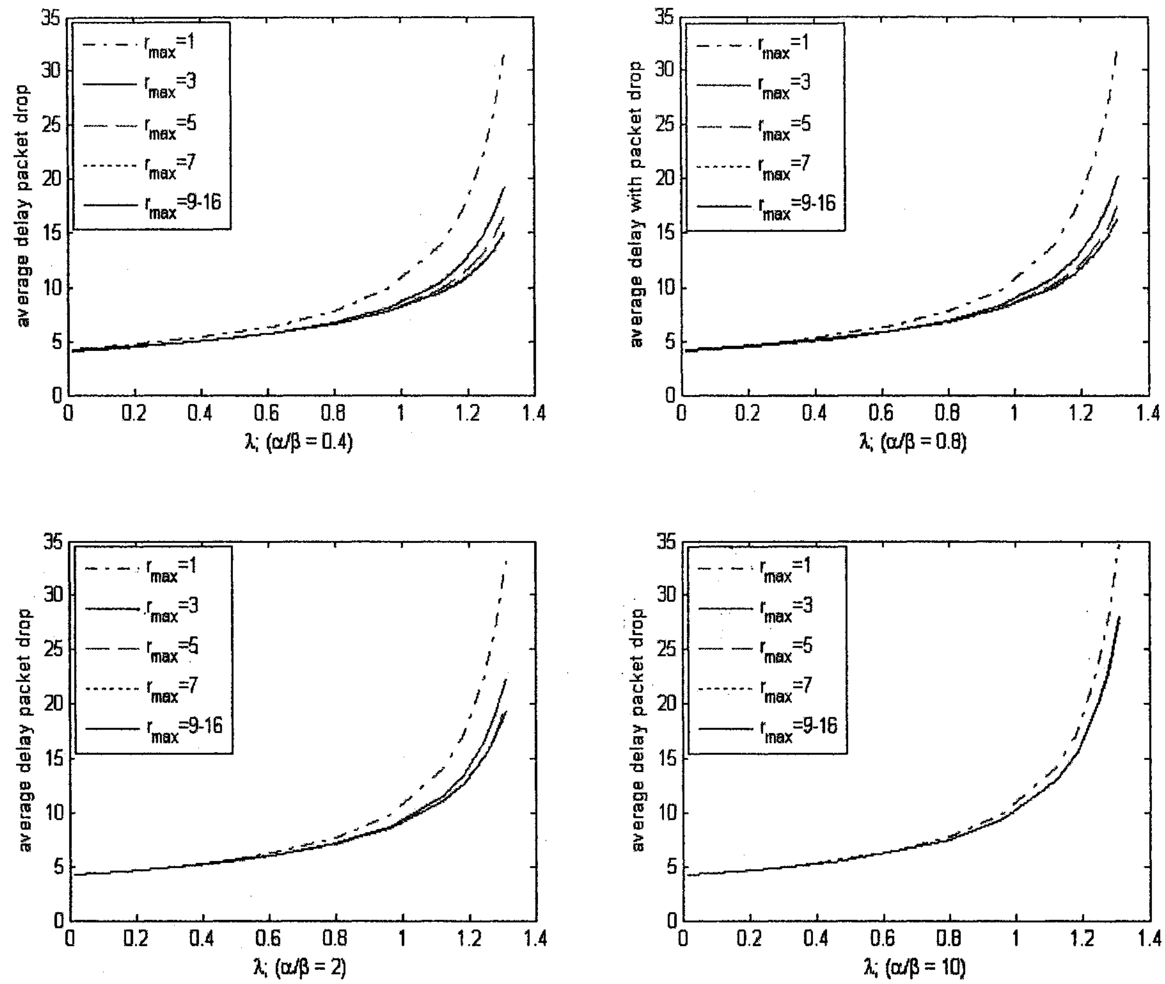


Figure 18: The average delay as a function of total arrival rate, λ, with r_{max} as a parameter with packet drop

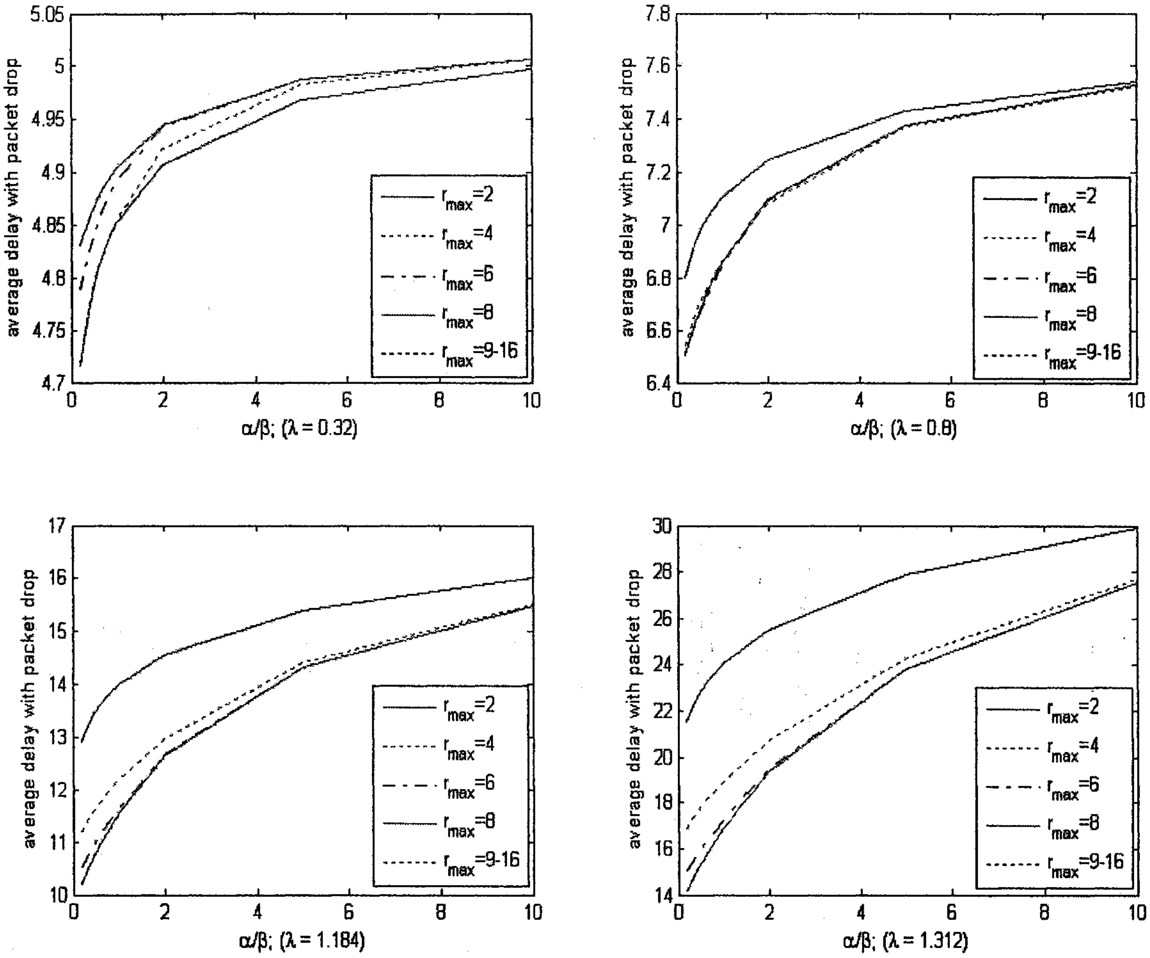


Figure 19: The average delay as a function of the sleep to wake up rate ratio α/β with r_{max} with packet drop

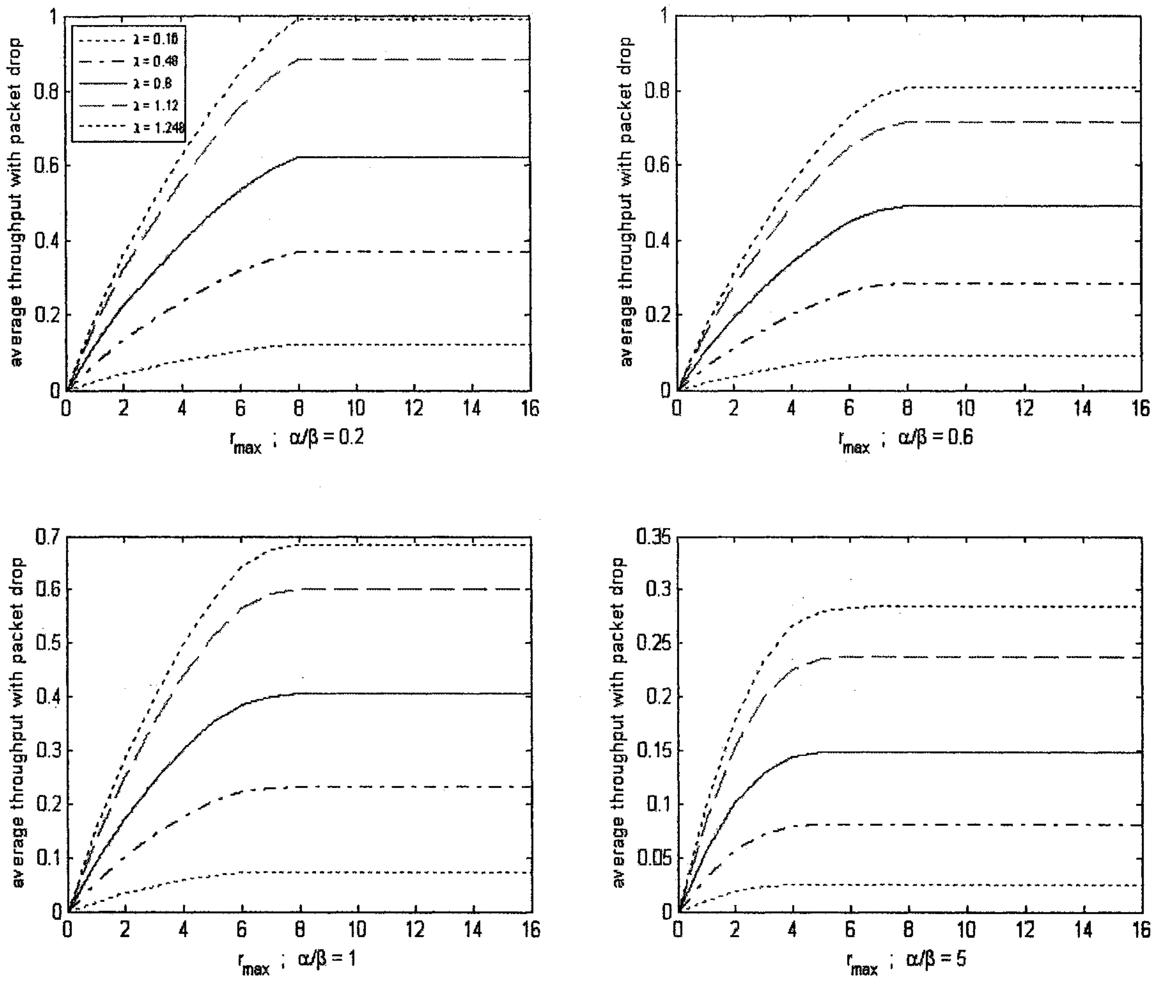


Figure 20: The average throughput as a function of r_{max} with total arrival rate as a parameter with packet drop

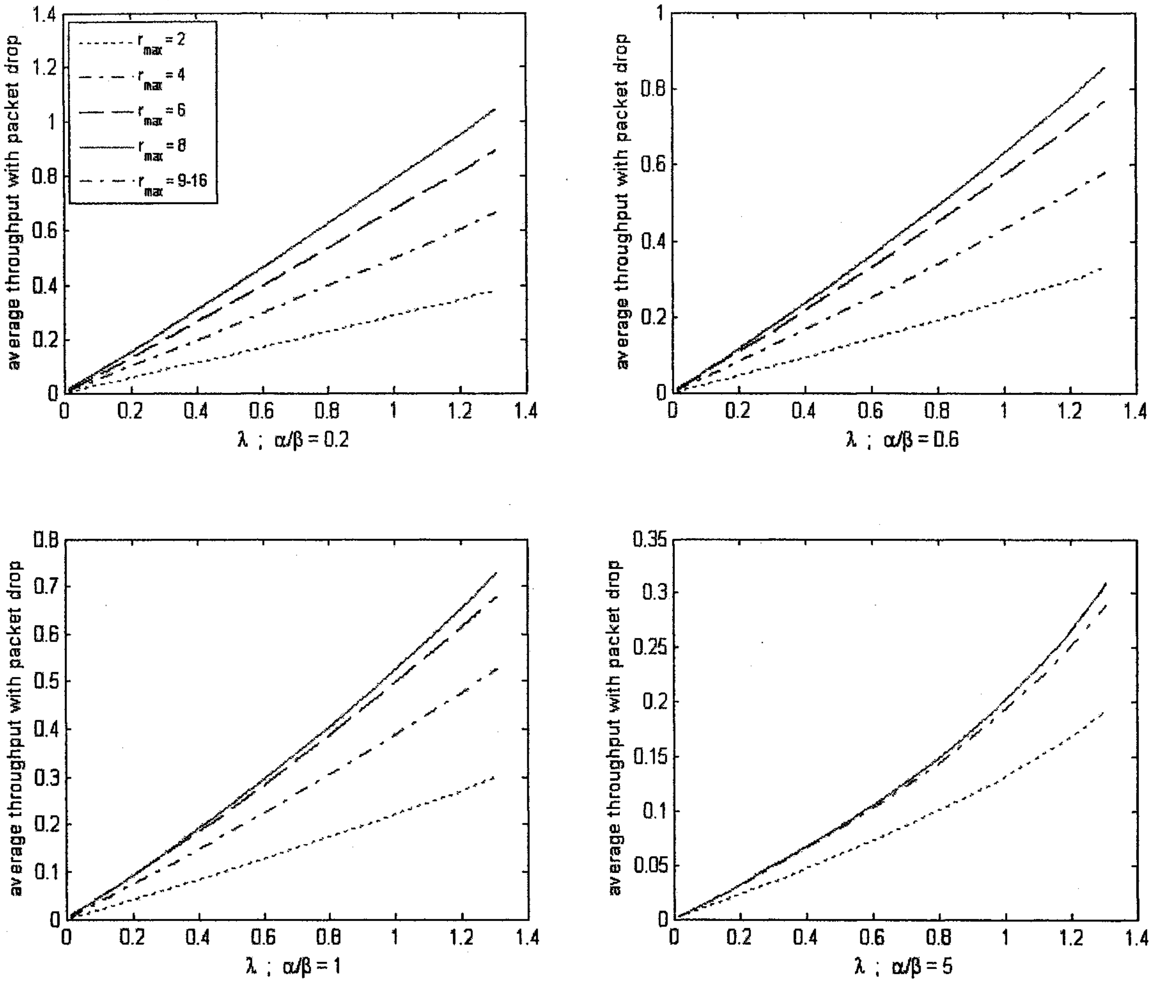


Figure 21: The average throughput as a function of the total arrival rate, λ, with r_{max} as a parameter with packet drop

4.4 Application of the Results in the Design of Wireless Sensor Networks

Next, we discuss how the results of the thesis may be used in the design of sensor networks. The main design parameters of the network are average sleep period, throughput, delay and the TDMA frame size in number of slots, r_{max}. As it has been shown above, as frame size increases average sleeping period of the nodes also decreases and as a result more traffic is admitted to the network. Though the network is handling higher amount of traffic, the mean packet delay is reduced due to increased availability of the nodes to relay traffic. As a result the average throughput of the network also increases. However, there is a value of the frame size, beyond which, there is no further improvement in the performance of the network. Thus this value of the frame size with the corresponding values of average throughput and delay provides the optimal operating point of the network.

CHAPTER 5:

CONCLUSIONS

5.1 Conclusions

The choice of MAC protocol is very important for wireless sensor networks because of energy constraints. In this thesis, we have studied the performance of TDMA based MAC protocol with timeslots reuse because of its energy efficiency. It is assumed that the nodes have two states, active and sleep modes. During the sleep state, a node releases its assigned slot. We have modeled this WSN with open network of queues with node breakdowns. The model also captures the reduction in the traffic load due to elimination of duplicated information.

The major results of the thesis are,

- Derivation of the joint distribution of queue lengths in the wireless sensor network.
- Determining number of performance measures:
    - The probability distribution of the number of active nodes
    - The blocking probability of node activation
    - The average sleeping period of selected nodes
    - The mean packet delay of the system
    - The average throughput of the network system

Finally, we show how these results may be used in the design of wireless sensor networks.

5.2 Future Challenges of Wireless Sensor Networks

There are still a large number of unexplored areas in wireless sensor networks, open research issues in all layers of the network architecture.

- Communication efficiency: Communication efficiency between sensor nodes depends on the transmission distance and the transmission power. Therefore, how to improve the communication efficiency in multi-hop routing is an important issue.
- Location awareness: Due to the dynamic feature of the wireless sensor networks, locating each node in the network is important. However, the cost of locating the nodes is very high, so how to minimize the cost and how to improve the precision of locating the node are big issues.
- Power consumption: This is still very important factor in wireless sensor networks. We have to save energy as much as possible in hardware design, MAC, and routing protocols, etc.
- Security and privacy: wireless sensor networks use wireless communication, so security and privacy problem is important.

REFERENCES

[1] F. Akyildiz et al., "Wireless sensor networks: a survey", *Computer Networks, Vol. 38*, pp. 393-422, March 2002.

[2] F. L. LEWIS, "Wireless Sensor Networks", *Smart Environments: Technologies, Protocols, and Applications*, ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.

[3] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, " A Survey on Sensor Networks", *IEEE Communications Magazine • August 2002*

[4] http://www.alertsystems.org

[5] Chee-Yee Chong, and Srikanta. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", *Proceedings of the IEEE, Vol. 91, No. 8, August 2003*

[6] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," *Proceedings of the Hawaii International Conference on Systems Sciences, Jan. 2000.*

[7] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, WA, August 1999.*

[8] G.J. Pottie and W.J. Kaiser, " Wireless Integrated Network Sensors", *Communications of the ACM, May 2000, Vol. 43, No. 5*

[9] J.M. Kahn, R.H. Katz, K.S.J. Pister, "Next century challenges: mobile networking

for smart dust", *Proceedings of the ACM MobiCom'99*, Washington, USA, 1999, pp. 271 - 278.

[10] I.F. Akyildiz, W. Su, "A power aware enhanced routing (PAER) protocol for sensor networks", *Georgia Tech Technical Report, January 2002.*

[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, "SPINS: security protocols for sensor networks", *Proceedings of ACM MobiCom'01*, Rome, Italy, 2001, pp. 189 - 199.

[12] C. Shen, C. Srisathapornphat, C. Jaikaeo, "Sensor information networking architecture and applications", *IEEE Personal Communications*, August 2001, pp. 52 - 59.

[13] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A.Chandrakasan, "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", *Proceedings of ACM MobiCom'01*, Rome, Italy, July 2001, pp. 272 - 286.

[14] J. Heidemann, F. Silva, C. Intanagonwiwat, "Building efficient wireless sensor networks with low-level naming", *Proceedings of the Symposium on Operating Systems Principles*, Banff, Canada, 2001.

[15] J. Rabaey, J. Ammer, J.L. da Silva Jr., D. Patel, Pico-Radio, "ad-hoc wireless networking of ubiquitous low energy sensor/monitor nodes", *Proceedings of the IEEE Computer Society Annual Workshop on VLSI (WVLSI'00)*, Orlanda, Florida, April 2000, pp. 9 - 12.

[16] S. Singh, M. Woo, and C.S. Raghavendra, "Power-aware routing in mobile ad hoc networks", *Proceedings of ACM MobiCom'98*, Dallas, Texas, 1998, pp. 181 - 190.

[17] IEEE Standard, 802.15.4™ Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

[18] Katayoun Sohrabi, Jay Gao, Vishal Ailawadhi, and Gregory J. Pottie, "Protocols for Self-Organization of a Wireless Sensor Network," IEEE Pers. Commun., Oct. 2000, pp. 16–27.

[19] IEEE Standard, 802.11™ Wireless Local Area Networks

[20] Phil Karn, "MACA: A new channel access method for packet radio," *Proceedings of the 9th ARRL Computer Networking Conference*, London, Ontario, Canada, Sept. 1990, pp. 134–140.

[21] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "MACAW: A media access protocol for wireless lans," *Proceedings of the ACM SIGCOMM Conference*, London, UK, Sept. 1994, pp. 212–225.

[22] Wei Ye, John Heidemann, and Deborah Estrin, "An energy-efficient MAC protocol for wireless sensor networks," *Proceedings of the IEEE Infocom*, New York, NY, June 2002, pp. 1567–1576.

[23] Suli Zhao, Ivan Seskar and Dipankar Raychaudhuri, "Performance and Scalability of Self-Organizing Hierarchical Ad Hoc Wireless Networks", WCNC 2004

[24] Swapnil Patil, "Performance Measurement of Ad-hoc Sensor Networks under Threats", WCNC 2004

[25] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking*, Boston, MA, USA, Aug. 2000, pp. 56–67, ACM.

[26] V. Rodoplu and T.H. Ming, "Minimum energy mobile wireless networks," *IEEE Journal of Selected Areas in Communications*, Vol. 17, No. 8, pp. 1333-1344, 1999.

[27] L. Li and J. Y Halpern, "Minimum energy mobile wireless networks revisited," *Proceedings of IEEE International Conference on Communications (ICC'01)*, Helsinki, Finland, June 2001

[28] C. F. Chiasserini, M. Garetto, "Modeling the Performance of Wireless Sensor Networks", *Proceeding of IEEE INFOCOM*, 2004.

[29] G.D. Nguyen, J. E. Wieselthier, and A. Ephremides, "Multiple-Access for Multiple Destinations in Ad-hoc Networks", Proc. WiOpt'03, Sophia Antipolis, France, Mar. 2003.

[30] Yalin Evren Sagduyu and Anthony Ephremides, "The Problem of Medium Access Control in Wireless Sensor Network," *IEEE Wireless Communications*, pp.44-53, Dec. 2004.

[31] L. Hoesel, T. Nieberg, J. Wu, P. Havinga, " Prolonging The Lifetime of Wireless Sensor Networks by Cross-Layer Interaction ", *IEEE Wireless Communications*, pp. 78-86, Dec. 2004.

[32] Cornelia Sauer and Hans Daduna, "Separable Networks with Unreliable Servers", *Proceedings of International Teletraffic Congress*, ITC 18, pp. 821-830, 2003.

[33] James R. Jackson *Operations Research*, Vol. 5, No. 4. (Aug., 1957), pp. 518-521.

[34] Leonard Kleinrock, *Queueing Systems, Volume II: Computer Applications*, John Wiley & sons

[35] F.P.Kelly, *Reversibility and Stochastic Networks*, Wiley, 1978