ENHANCED ROUTING PROTOCOL FOR GRACEFUL DEGRADATION IN WIRELESS SENSOR NETWORKS DURING ATTACKS

A Thesis by

Preetha Radhakrishnan

Bachelor of Engineering, University of Madras, Chennai, 2003

Submitted to the Department of Electrical and Computer Engineering
and the faculty of the Graduate School of
Wichita State University in partial fulfillment of
the requirements for the degree of
Masters of Science

December 2005

ENHANCED ROUTING PROTOCOL FOR GRACEFUL DEGRADATION IN WIRELESS SENSOR NETWORKS DURING ATTACKS

I have examined the final copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Electrical Engineering.

_____

Dr. Ravi Pendse, Committee Chair

We have read this thesis and recommend its acceptance:

_____

Dr. Kameswara Rao Namuduri, Committee Member

_____

Dr. Krishna Krishnan, Committee Member

DEDICATION

To my Mother

ACKNOWLEDGEMENTS

My graduate study in Wichita State University has been an incomparable learning experience both academically and individually. I thank my friends in India for supporting me in all my endeavors and encouraging me to be what I am today. With out them my MS would have remained a dream. I am thankful to each and every one who directly or indirectly helped me to achieve the requirements for completing my MS.

I extend my gratitude to my advisor, Dr. Ravi Pendse, for his guidance and support both academically and personally. I enjoyed his lively lectures and always admired his charismatic personality. I am thankful to my thesis committee members, Dr. Kameswara Rao Namuduri and Dr. Krishna Krishnan for sparing their time in reviewing this thesis report.

Special thanks are extended to doctoral students Nagaraja Thanthry, Sabeeh Ali, Amarnath Jasti and Murali Krishna Kadiyala. It is with their guidance and suggestions this thesis dissertation has become possible.

I sincerely thank my Grand-mother P.S.Padmavathy, who was gracious to bring me up and sponsor my education throughout my life. I am grateful to my Mother for her unconditional love and limitless affection. My special thanks to my Brother and Sister for being the most wonderful siblings anyone could ever have. I thank my little sororal niece for rejuvenating my days with her smile. I am obliged to my Husband Sanjiv for being so caring and tolerant towards me. Without their support, this venture would not have been possible.

Most of all, I thank the Almighty for being graceful to me my entire life. With out his charm I could not have reached this position.

ABSTRACT

With the deployment of Sensor networks gaining some popularity, researchers are now focusing on solving the issues concerned with making sensor networks more feasible and viable. As Sensor networks have various constraints in terms of limited resources available, not many researchers come forward to work on the security issues for this stringent environment. Lately, it has been realized that these sensor networks which have found application in many trivial situations need to be secured. And though this security comes with the expense of some portion of its resources, it has been proved to be essential for the survival of sensor networks to serve their purpose.

LEACH (Low Energy Adaptive Clustering Hierarchy) is an architecture for remote microsensor networks that combine the concept of energy efficient cluster based routing and media access, together with application specific data aggregation to achieve good performance in terms of system lifetime and latency. This approach has been proved to improve system lifetime by an order of magnitude, compared to general purpose approach when the node energy is limited.

Though LEACH has several good qualities which have been widely accepted for various researches in the field of WSN, it has a hitch attached to it like any other WSN when we consider security factor. As control is distributed through out the network of making self organization possible, the cluster head nodes play an important role in the network. Hence they become a very attractive vulnerable point to the attackers. If a laptop class malicious node manages to take up this powerful cluster head position, the networks performance can be

devastated within no time, without any effort. In this thesis, we propose an enhancement to LEACH in order to secure this powerful cluster head position from being easily occupied by a trespasser node. Our enhancement also restricts the malicious node from using its superiority of very high power source and other resources to exploit the sensor network. We have also proved that the increase in the delay and energy spent for protecting the cluster head election by encryption and decryption, is affordably less when compared to the energy already being spent in a node. However, this tradeoff is natural and necessary in order to achieve the minimal security of Wireless Sensor Network so that they serve their purpose in an uninterrupted manner.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF ABBREVIATIONS

ADV	Advertisement
AODV	Ad-Hoc On-demand Distance Vector
CDMA	Code Division Multiple Access
CH	Cluster Head
CSMA	Carrier-Sense Multiple Access
CTS	Clear to send
DSDV	Destination-Sequenced Distance Vector
DSP	Digital Signal Processing
E	Energy
Etransmit	Transmission Energy
Eq	Equation
FDMA	Frequency Division Multiple Access
ID	Identifier
Join-REQ	Join Request
LEACH	Low Energy Adaptive Clustering Hierarchy
MAC	Media Access Control
MTE	Maximum Transmission Energy
N-CH	Non Cluster-Head
PC	Personal Computer
PDA	Personal Digital Assistant
PEGASIS	Power-Efficient Gathering in Sensor Information Systems

RTS	Request to send
SDMA	Space Division Multiple Access
SPIN	Sensor Protocol for Information via Negotiation
SWAN	Self-organizing Wireless Adaptive Network
T	Time
TDMA	Time Division Multiple Access
TEEN	Threshold sensitive Energy Efficient sensor Network protocol
WLAN	Wireless Local Area Network

CHAPTER 1

INTRODUCTION

1.1 Overview

Networking is the term used to refer to hardware and software that connect computers, in order to allow them to communicate with one another. This inter connection can be achieved through cabling, or wireless network operating systems. Hence, the two main types of networking are Ethernet networking and wireless networking. Today both of these techniques are popularly used in order to link multiple computers with each other and to the internet.

Though Ethernet is the fastest home-networking technology at present, it has other drawbacks in terms of installation expenses, scalability and convenience. Wireless networking meets these short comings and has paved way to its present popularity.

Wireless Networking is on the rise and continues to add a whole new level of convenience to networking. It has remarkably reduced the set-up cost and maintenance expenses of a computer network. The mushroomed usage of wireless devices like cellular phones, laptops, pagers and PDA's show that the wireless technology has become a part of our day-to-day essentials. These wireless networks can operate in two different modes namely, infrastructure mode and Adhoc (Infrastructure-less) mode.

Infrastructure mode can be used to bridges a wireless network to a wired Ethernet network or to expand an existing wireless network. It supports a central connection point

for the WLAN clients. The wireless access point serves as the central WLAN communication station. Ad-Hoc mode is the method where wireless devices directly communicate with each other. Devices operating in ad-hoc mode can discover other wireless devices within their range and communicate with them in peer-to-peer fashion without any need for other central devices like access points. This is typically used by two PCs that try to communicate with one another, so that one can share the other's resources like the Internet connection.

The serious challenge faced in designing wireless and mobile systems is the resources available to them like the bandwidth, memory capacity and energy are very limited when compared to their wired counterparts. Especially when dealing with sensor networks, once these sensor nodes are deployed, they are generally inaccessible for the user to replace their resources such as batteries. To meet such limitations several protocols have been proposed to achieve reasonable life-time of the network with the available energy supply. Sensor networks have recently gained popularity in several applications such as habitat sensing, seismic monitoring, battlefield surveillance, monitoring vehicular traffic, object tracking and many more. The conventional protocols like direct transmission, minimum transmission energy, multi-hop transmission and clustering have several short comings that have been overcome in the latest mechanisms. Based on the application for which these sensor networks are designed to be used, researchers have proposed various application specific protocols like LEACH, SPIN, LEACH-C, LEACH-F, PEGASIS, et al that focus on enhancing individual features critical to their application.

LEACH (Low-energy Adaptive clustering Hierarchy):

LEACH deploys clustering methodology to proficiently pass the queries and collect sensor readings to and from all the other nodes in the network. It assumes that every node in the network is capable of directly reaching the base station with adequately high powered transmissions. As these high powered single hop transmission directed to the base station consumes more power, it proves to be in efficient while considering the redundancy that usually occurs in sensor networks. Hence, LEACH organizes nodes into several clusters where one node from every cluster acts as the *cluster-head*. The non-cluster head nodes first send the readings to their cluster-head, and the cluster-head transmits the aggregate of the data from all its "children" to the base station. These nodes chosen as cluster-heads would quickly run out of energy and die if they continue to serve as cluster-heads for ever. Thus, LEACH deploys randomized rotation of nodes serving as cluster-heads in order to evenly distribute energy consumption over all nodes in the network. LEACH operation is split up into several rounds, and every round has a set-up phase and a steady-state phase. In the beginning of the set-up phase, each node probabilistically decides whether or not to be a cluster head based on its remaining energy and a globally known desired percentage of cluster heads. Each node electing itself as a cluster-head broadcasts an advertisement message (Hello message) announcing its intention. Non-cluster head nodes receive possibly numerous advertisements and choose one of the clusters to join based on the largest received signal strength of the advertisement from the corresponding cluster-head. Nodes inform the cluster-head of the cluster they intend to join, and each cluster-head sends back a TDMA schedule for

sending data to it for each node in its cluster. In the steady-state phase, each cluster-head waits to receive data from all nodes in its cluster and then sends the aggregated result to the base station. As the actual data transmission takes place during the steady-state phase, this phase is preferably kept longer than the set-up phase.

Such sensor networks involving various protocols like LEACH find their application in different areas where integrity, and confidentiality of data is very essential, it is important to focus on the kinds of security attacks these sensor networks are prone to and the way in which they can be overcome with out affecting the function of the network and its life time. The many different types of attacks to which LEACH protocol is exposed to are mentioned by Chris Karlof and David Wagner [2]. This thesis dissertation introduces a method to protect the Sensor network against the HELLO flood attack with out affecting the life time of the sensor node and conserving their resources as much as possible. This HELLO flood attack is proved to be more devastating to the LEACH protocol by misusing the powerful Cluster head privilege given to the elected Cluster Head nodes.

1.2 Problem Statement

This part of the introduction discusses about the area of vulnerability found in the LEACH and emphasizes on why it should be protected. In LEACH a cluster head is being elected by its nodes based on the signal strength of the broadcast that is being received by them. If a laptop-class foe participates in the set-up phase and sends an advertisement with enormously high signal strength to all the nodes in the network it can disable the entire network. Due to the large signal strength of the advertisement, every

node is likely to choose the adversary as its cluster-head. Once it becomes the cluster-head, the adversary can selectively forward the data transmissions that take place through her and hence successfully disable the rest of the network. Thus a laptop-class rival can attack the entire network by attacking only a small number of nodes that are supposed to behave as the cluster head. This HELLO flood attack can further lead to selective forwarding attack and sink-hole attack. In selective forwarding attack the rival node ensures that all the traffic in its vicinity passes through her which is a typical scenario in case of LEACH which is a clustering protocol. The adversary can use the same technique to mount a selective forwarding attack on the entire network using only a small number of nodes if the target number of cluster heads or the size of the network is sufficiently small. Even other clustering protocols and protocols extending LEACH such as TEEN and PEGASIS are also susceptible to attacks analogous to those described here.

1.3 Proposed Solution

Our goal is to protect the sensor network form a laptop-class adversary by preventing it from taking part in the set-up phase. Secondly, even if they make an attempt to take part in the set-up phase they should not be successful in being elected as the cluster head. If they participate in the set-up phase they are capable of disabling the entire network by transmitting Hello packets of very high intensity during the set-up phase. By sending out these hello packets with very high transmission power the adversary could convince even all the nodes in the network as the best potential cluster-head for them. Since the nodes choose their cluster heads based on the signal strength of the Hello packets received during the set-up phase it is possible to assign a threshold level for this

signal strength which could be the maximum possible transmission power that is achievable by a sensor node of the kind that we have implemented in the network. Since we know the nature of the nodes deployed we can determine the maximum possible signal strength with which a broadcast can be received by their neighbors even if they where right next to the broadcasting node. By setting up this value as the threshold upper limit, any packet received with unbelievably high signal strength should be discarded and the corresponding source node should be marked as malicious and eliminated from the process for election for the Cluster head.

In order to provide a supplementary level of security to the network this protocol deploys minimal encryption to encrypt only the header of HELLO packets instead of encryption all the packets traversing the channel. This protects the network performance from being devastated instantly as the cluster head election process is being secured. Though this minimal encryption would cause some amount of delay, consume a few processor cycles and energy it is proved to be vital in order to secure the network. This trade-off is acceptable in order to protect functionality of the sensor network. And as all the encryption and decryption is going to take place only in the setup phase which consumes very negligible energy when compared to the steady state phase securing this phase of the protocol is not expected to introduce any significant overhead.

1.4 Thesis Organization

The remainder of this thesis report is organized as follows: Chapter 2 discusses the basic concept of Wireless Sensor Network and how it differs from the other types of networks. It also gives an over view of different routing protocols that have been

proposed for the sensor networks. Chapter 3 explains the LEACH protocol operation in detail because, in order to understand the mechanism suggested in this dissertation, understanding the set-up phase operation of LEACH is very important. In Chapter 4, the enhancement proposed to LEACH in order to provide a first level security to its operation is introduced. Also all the assumption related to this dissertation are mentioned here. The next Chapter 5 explains the mathematical model derived for the proposed enhancement with several equations and their explanations. The last Chapter 6 discusses the validity of our proposed mechanism with various graphs obtained by simulating the values for the equations derived in the mathematical model. These graphs are analyzed and the reasons for the graphs obtained are also analyzed here.

CHAPTER 2

LITERATURE SURVEY

This chapter gives the gist of various research papers and articles read by the author in order to gain the background knowledge required for this thesis dissertation. The four subsections in this chapter discuss about the operation of wireless sensor networks, how LEACH protocol works, its vulnerability to security attacks, and the existing security protocols for sensor networks respectively.

2.1 Wireless Sensor Networks (WSN)

Wireless sensor network is an up and coming discipline in the field of networking. Recent developments in the field of signal processing and digital communication have led to the emergence of microsensors of great competence at very low cost and small size. As these sensors are designed to be deployed in remote localities, in very large numbers and might even be dispersed from air crafts, they are required to be kept cheap and still efficient. Collection of such integrated microsensor nodes incorporating sensing, signal processing and wireless communication capabilities combine to form a wireless sensor network.

Sensor networks are the key to gathering information needed by smart environments wherever they are implemented. With their flexibility, fault tolerance, high sensing fidelity, low cost and rapid deployment characteristics, they find their application in various fields like in the military for enemy tracking and battle field surveillance, for

civil applications like habitat monitoring, environment observation, industries, shipboard, transportation systems automation seismic monitoring and more where they are located very close to or even in the area where any phenomenon is to be observed. Recent terrorist and guerilla warfare countermeasures require distributed networks of sensor nodes that have self-organizing capabilities and can be conveniently deployed from aircrafts. Hence, running wires or cabling turns out to be unfeasible in such applications. The tiny sensor nodes dispersed in the area under observation mostly operate unattended. These nodes sense the atmospheric conditions or detect motion as per the requirement of their application and the sensed information is communicated to a sink, which is termed as the base station. This base station in turn transmits the data to the remote user, with the help of satellite or internet technology.

2.1.1 Protocol stack

The protocol stack used by base station and sensor nodes is shown in Fig [2.1]. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane and task management plane.

The physical layer should meet requirements like robust modulation, transmission and receiving mechanisms. The MAC layer should be capable of collision detection and use minimal power. The network layer is responsible for routing the information received from the transport layer. The application layer software depends on the deployment and

use of sensor networks. The power management plane manages power utilization by the nodes. A sensor node may decide to turn itself off periodically, when it is not being used. If the sensor nodes are mobile, mobility management is responsible for the movement pattern. The task management plane schedules the sensing and forwarding responsibilities of the sensor nodes.

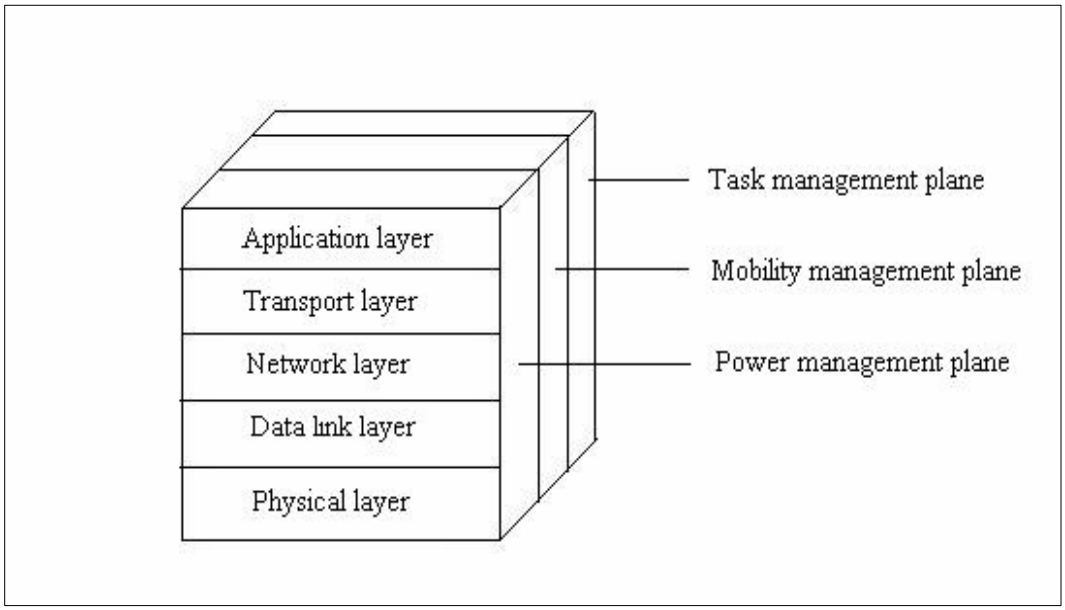

Figure 2.1: Sensor Network Protocol Stack

Designing a network protocol for such wireless devices should meet the limitations [1] like limited channel bandwidth, limited energy, electromagnetic wave propagation, error-prone channel, time varying conditions and mobility. There are general ideas that can be used to overcome these limitations. Low-energy protocols help extend the limited node energy. Power control can be used to combat the radio wave attenuation. A transmitter can set the power of the radio wave, such that it will

be received with an acceptable power level. Link-layer protocols and MAC protocols can be used to combat channel errors. Adaptive routing, MAC and link-layer protocols can be used to overcome the time-varying conditions of the wireless channel and node mobility.

2.3 Media Access Control (MAC) Protocols

The MAC protocols can be classified in to two namely fixed-assignment protocols and random access methods. Fixed-assignment MAC protocols allocate each user a given amount of bandwidth, either slicing the spectrum time in TDMA, frequency in FDMA, code in CDMA or space in SDMA. Since each node is allocated an exclusive part of the spectrum, there are no collisions among the data. However, fixed-assignment schemes prove to be inefficient when all nodes do not have data to send, since scarce resources are allocated to nodes that are not using them. Random-access methods on the other hand, are contention-based schemes, where nodes that have information to transmit must try to obtain bandwidth while minimizing collisions with other node's transmissions. These MAC protocols are more efficient than fixed-assignment MAC protocols.

A. TDMA- Time-division multiple access

In this protocol, each node is given the entire bandwidth for a certain time-slot. During this time-slot; no other node should transmit data.

B. FDMA - Frequency-division multiple access

In this protocol_ each node is given a slice of bandwidth and continuously sends data

within this bandwidth slice. No other node should transmit in the frequency slice given to a particular node.

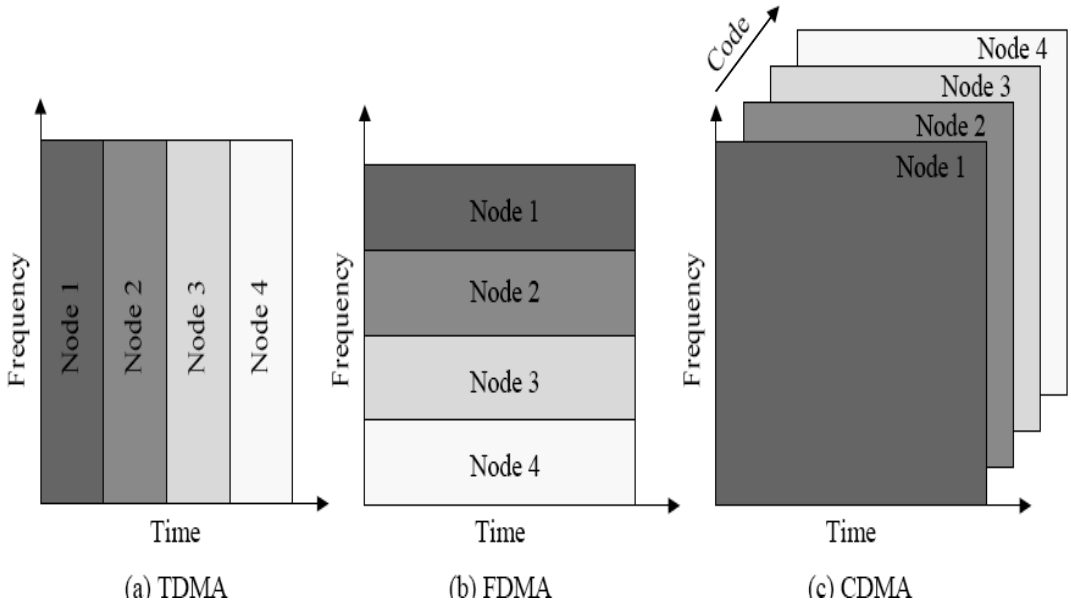

Figure 2.2: Representational diagram of MAC Protocols *(a) TDMA, (b) FDMA, (c) CDMA*

C. CDMA- Code division multiple access (CDMA)

In this protocol, each node spreads its data using a unique pseudo-random noise sequence. Therefore all nodes use the entire bandwidth at all times. However they suffer from possible collisions of the data when nodes have bursty traffic. Here all nodes are contending for the resources leads to collision. Often protocols use a hybrid approach like combining TDMA and FDMA by allocating a certain time and

frequency slot for each node as shown in the figure 2.2. MAC protocols can be evaluated in terms of energy dissipation, fairness, and throughput, where the protocol is typically optimized to minimize energy dissipation, give each node its fair share of the bandwidth and achieve high throughput.

2.4. Routing protocols

The two broad classifications of routing protocols for wireless networks are multi-hop routing protocols and clustering (cellular) protocols. The distance vector and link-state protocols of wired networks have been incorporated in wireless networks with some alteration as destination-sequenced distance vector (DSDV) and ad hoc on-demand distance vector (AODV) routing protocols [6], [7]. These protocols have some drawbacks when used for wireless networks. The periodic messages exchanged to validate the routes cause congestion and also consume energy leaving the battery drained. Dynamic Source Routing (DSR) can be used to overcome this drawback as it creates routes only on-demand basis [4]. This minimizes the amount of overhead needed in creating routes at the expense of latency, in finding a route only when it is needed. These are ad hoc routing protocols that are self configuring.

2.4.1. Minimum-energy routing protocols

Researchers have come up with “minimum-energy” routing protocols to try to prolong the lifetime of portable devices in a wireless network. [12] proposes a strategy for choosing multi-hop routes to minimize the power dissipated in the nodes along the route. This is achieved by using an intermediate node as a hop if and only if it minimizes

the total energy spent, compared to the energy spent when not using this middle hop node. A similar idea is proposed in [9], where the authors make a note of interference that takes place in a wireless network, due to transmission between neighboring nodes and degrading the network performance in turn. Hence routes are chosen to minimize interference which would in turn minimize energy dissipation.

2.4.2. Self-Organizing Wireless Adaptive Network (SWAN) protocols

The Self-Organizing Wireless Adaptive Network (SWAN) protocol [11] uses dynamic topology management with power control to deform the network gradually instead of having the network periodically broken down and rebuilt. This allows user data to experience a minimum amount of delay and prevent outages due to network recovery functions.

2.4.3. Power-aware routing protocols

"Power-aware" routing protocols for wireless networks have been proposed in [13]. These protocols, select the optimal routes based on the energy of each node along the path. High-energy nodes that constitute longer routes are preferred to low-energy nodes along the shorter routes. This helps to avoid hotspots in the network, and evenly distributes the energy dissipation.

2.4.4. Minimum transmission energy (MTE) routing

In "Minimum transmission energy" (MTE) routing discussed in [28, 84] a node A will transmit to node C through node B if and only if

$$E_{transmit}(d = d_{AB}) + E_{transmit}(d = d_{BC}) < E_{transmit}(d = d_{AC}) \quad \text{--- (1)}$$

2.4.5. Clustering Approach

Clustering approach is similar to the technique used in cellular networks. In this approach, nodes send their data to a central cluster-head which forwards the data to the base station. Clustering facilitates reuse of bandwidth and thus increases the system capacity. This approach enables better resource allocation and helps improve power control.

2.4.6. SPIN (Sensor Protocol for Information Dissemination via Negotiation)

SPIN [41] is a family of protocols to disseminate information in a wireless microsensor network. In SPIN, large data messages are named using high-level data descriptors called meta-data. Nodes use meta-data negotiation to eliminate the transmission of redundant data throughout the network. As nodes make their routing decisions on the basis of application-specific information about the data, great energy-savings is achieved.

CHAPTER 3

LEACH

3.1 Architecture

LEACH [1] is an architecture for remote microsensor networks that combines the ideas of energy efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency and application perceived quality. This approach improves system lifetime by an order of magnitude compared to general purpose approaches when the node energy is limited. It is designed for applications where an end-user wants to monitor an environment remotely. In such a condition, the data from the individual nodes must be sent to a central base station, which is generally located far-off from the sensor network. The end-user then accesses the data from the base station. Leach emphasizes on eliminating redundant, long distance communication that takes place between the nodes and the remote base station. To achieve this it deploys distributed cluster formation, local computation, data compression and random cluster head rotation techniques.

The protocol architectures for microsensor networks described in [1] were designed in the background of the μAMPS (Micro-Adaptive Multi-domain Power-aware Sensors project).The architecture for a μAMPS node is shown in Figure ____ .The first version of the μAMPS node contains the StrongARM (SA1100) microprocessor running a lean version of the RedHat eCos operating system for implementation of DSP algorithms and communication protocols [31]. The μAMPS nodes sense data using either a sensor, filters and digitize the data, performs signal processing functions on it and

finally transmits the data. On the receiving end, the nodes receive data, perform signal processing functions and transmit a response. Sensor network protocols can be implemented within this μAMPS framework. The use of the SA1100 processor allows the μAMPS nodes to be easily programmed to run different protocols and enables monitoring of the energy dissipation required for the various functions performed in the protocol.

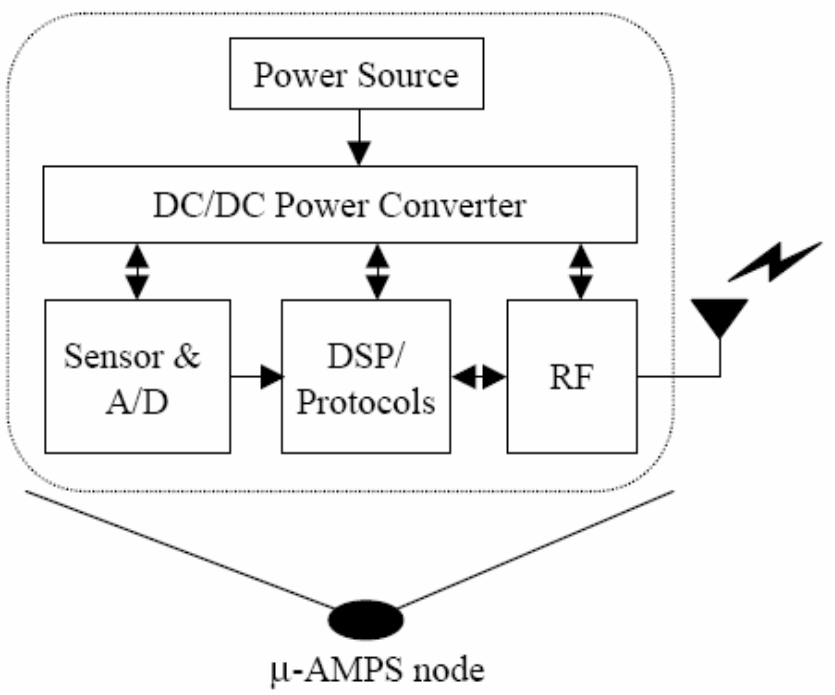

Figure 2.3: Microsensor Node Architecture

The limited battery capacity of microsensor nodes and the large amount of data that each node may produce interprets to the need for high application-perceived performance at a minimum cost, in terms of energy and latency. Cross-layer or application-specific

protocol architecture meets these specifications by exposing lower layers of the protocol stack to the requirements of the application. To meet the requirements of wireless microsensor a network, LEACH which is application-specific protocol architecture was developed Figure (2.3). LEACH is a clustering-based protocol that includes features like

- randomized-adaptive- self-configuring cluster formation
- localized control for data transfers
- low-energy media access and
- application specific data processing such as data aggregation

LEACH has been designed for an application that typical microsensor networks support is the remote monitoring of an environment. Since every individual node's data are associated in a microsensor network the end-user only needs a high-level function of the data and not all the redundant data form every node in that area. In LEACH, the nodes organize themselves into clusters where one node is elected as the cluster-head. All non-cluster-head nodes transmit their data to their cluster-head, while the cluster-head node performs signal processing functions like data aggregation and transmit it to a remote sink which is the base station. Thus, being a cluster-head node is much more energy-consuming than being a non-cluster-head node. In a situation where all nodes have limited energy, if the cluster-heads were chosen a priori and fixed throughout the system lifetime, as in a static clustering algorithm, the sensor nodes playing the role of a cluster-head would quickly use up their inadequate energy. Once the cluster-head's energy is exhausted, it becomes ineffectual.

Therefore, when a cluster-head node dies all the nodes in its cluster lose contact

with the remote base station. In order to avoid this LEACH incorporates randomized rotation of the high-energy cluster-head position so that all nodes take up the cluster head responsibility in rotation basis. This avoids draining of the battery of a few sensors in the network. In this way, the energy overhead associated with being a cluster-head is evenly shared among all the nodes. The motive of media access in LEACH is to reduce energy dissipation in the non-cluster-head nodes [1]. As the cluster-head node knows all the cluster members it creates a TDMA schedule that allots an exact time slot for each node to transmit its data. Thus the nodes may remain in sleep state with internal modules powered down as long as possible. This also prevents intra-cluster collisions.

3.2. Operation of LEACH

The operation of LEACH is divided into two rounds. Each round begins with a set-up phase where the clusters are structured, followed by a steady-state phase where several frames of data are transferred from the nodes to the cluster-head and on to the base station, as shown in Figure2.4.1In order to minimize the set-up overhead, the steady-state phase is kept longer than the set-up phase.

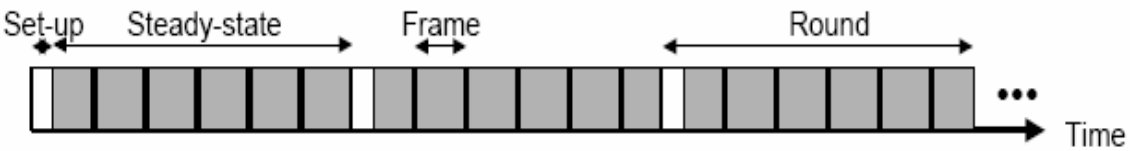

Figure 2.4.1 Time-line of two phases in LEACH operation. Adaptive clusters are formed during the set-up phase and data transfers occur during the steady-state phase.

The nodes are time-synchronized in order to start the set-up phase simultaneously.

3.2.1 Set-up Phase

3.2.1(A). Cluster Formation:

LEACH forms clusters by using a distributed algorithm, where nodes make autonomous decisions without any centralized control, hence known as self-configuring. Thus long-distance communication with the base station is avoided and distributed cluster formation takes place with out any knowledge of the exact location of any of the nodes in the network. In addition, no global communication is needed to set up the clusters and nothing is assumed about the current state of any other node during cluster formation. Hence good clusters formation out of the nodes is achieved purely via local decisions made autonomously by each node.

3.2.1(B). Cluster-head selection:

The cluster-head is selected such that

- There are k number of clusters during each round
- Energy dissipation is evenly distributed among all the nodes so that no node is over utilized.
- All nodes serve as cluster-heads approximately the same length of time (as all nodes are assumed to start with the same amount of energy).
- The cluster-head nodes should be spread throughout the network (so that the non-cluster-head nodes need not send their data to a long distance).

In LEACH, sensors elect themselves to be cluster-heads at the beginning of round r +1 with a certain probability Pi (t), such that the expected number of cluster-head nodes for

this round is k. Thus

$$E[\#\ \mathrm{CH}] = \sum_{i=1}^{N} P_i(t) * 1 = k \qquad \text{--- (2)}$$

Where, N = total number of nodes in the network.

t= time at which the round starts such that

Hence the probability for each node i to be a cluster-head at time t is given by

$$P_i(t) = \begin{cases} \frac{k}{N - k*(r \bmod \frac{N}{k})} & : \quad C_i(t) = 1 \\ 0 & : \quad C_i(t) = 0 \end{cases} \qquad \text{--- (3)}$$

Where r is the number of rounds that have passed and $Ci(t)$ = 0 if node i has already been a cluster-head in the most recent (r mod N/k) rounds and 1 if not. Therefore, only nodes that have not already been cluster-heads recently and which most likely have more energy available than nodes that have recently performed this energy-intensive function become cluster-heads for round r+1.The expected number of nodes that have not been cluster-heads in the first r rounds is N -k * r. After N/ k rounds, all nodes are expected to have been cluster-head once_ following which they are all eligible to perform this task in the next sequence of rounds.

Therefore, the total number of nodes that are eligible to be a cluster-head at time t is given by

$$\sum_{i=1}^{N} C_i(t) \qquad \text{--- (4)}$$

Hence,

$$E[\sum_{i=1}^{N} C_i(t)] = N - k * (r \bmod \frac{N}{k}) \qquad \text{--- (5)}$$

Expected number of clusters per round is given by

$$
\begin{aligned}
E[\#\ \mathrm{CH}] &= \sum_{i=1}^{N} P_i(t) * 1 \\
&= (N - k * (r \bmod \frac{N}{k})) * \frac{k}{N - k * (r \bmod \frac{N}{k})} \\
&= k
\end{aligned}
$$

3.2.1(c) Cluster set-up

The cluster-head nodes after being elected should inform that they are the cluster-head for the current round .to other nodes in the network. So they send out a broadcast advertisement message (ADV) using a non-persistent carrier-sense multiple access (CSMA) MAC protocol. This ADV is a small message containing the node's ID and a header that indicates that this message is an announcement message. This message is broadcast to all the nodes in the network in order to ensure that all nodes hear the advertisement. This eliminates collisions when CSMA is used as there is no hidden terminal problem and also ensures that the cluster-heads are evenly spread out. The power of the advertisement messages is kept high so that nodes on the extreme edges hear the ADV and participate in the set-up round. As these advertisement messages are small, the increased power to reach all nodes will not be burdening the nodes.

The non-cluster-head nodes choose the cluster-head that requires minimum communication energy, based on the signal strength of the advertisement received and then join the corresponding cluster. In case of ties, a random cluster-head is chosen. Once the cluster-head is decided each node transmits a join-request message (Join-REQ) to the chosen cluster-head using a non-persistent CSMA MAC protocol. Join-REQ is a short

message that consists of the node's ID, the cluster-head's ID and a header. Since the node has an idea of the relative power needed to reach the cluster-head based on the received power of the advertisement message it adjusts its transmit power to this level

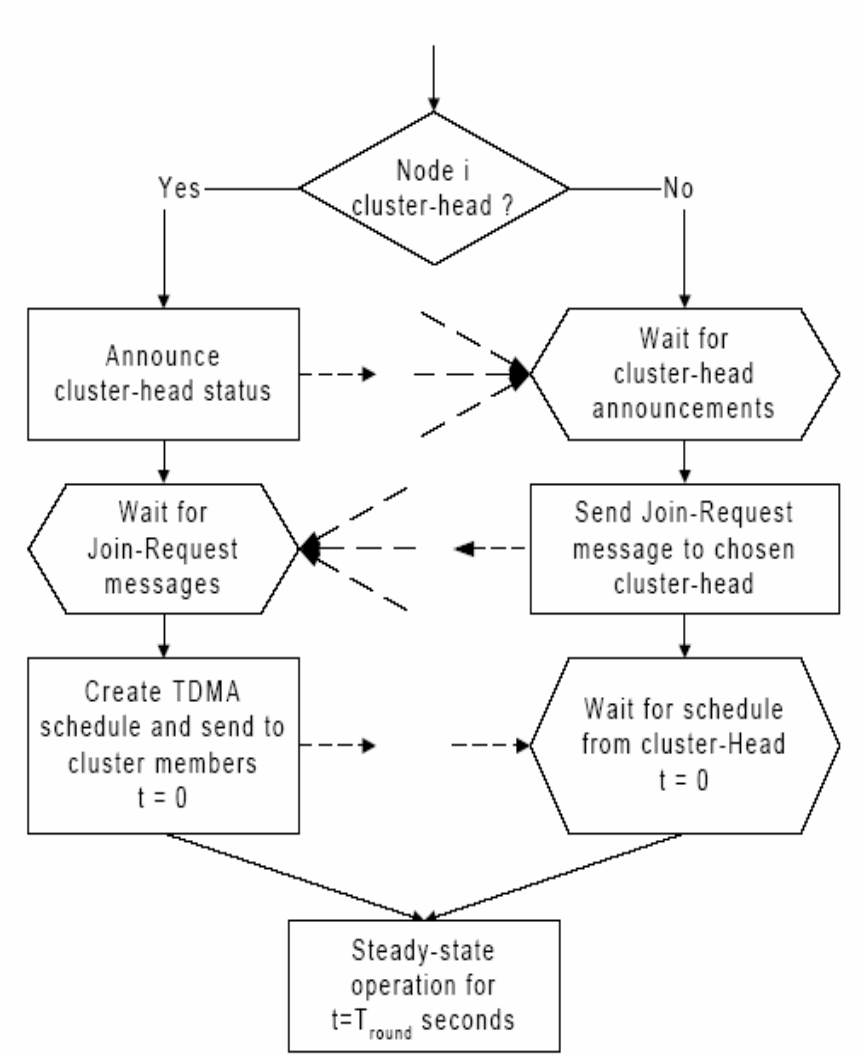

Figure 3.2.1: LEACH Protocol Setup Phase

However, this approach suffers from hidden terminal problem. To over come this

problem in an energy efficient way, the transmit power of the join-request messages is increased rather than deploying request-to-send (RTS) and clear-to-send (CTS) mechanism that uses high power transmissions to unknown number of potential cluster members.

In Leach, as the cluster-heads coordinate the data transmissions in their cluster, they set-up and transmit a TDMA schedule to the nodes in their cluster. This ensures that there are no collisions among data messages and also allows the radio components of non-cluster-head nodes to be turned on only during their transmit time. Once all nodes know their TDMA schedule, the set-up phase is complete and is followed by the steady-state operation.

3.2.2 Steady State Operation

The steady state operation of the LEACH protocol remains un-affected due to the encryption and decryption process. The enhancement is only confined to the setup phase as the main aim of this idea is to protect the cluster-head election process.

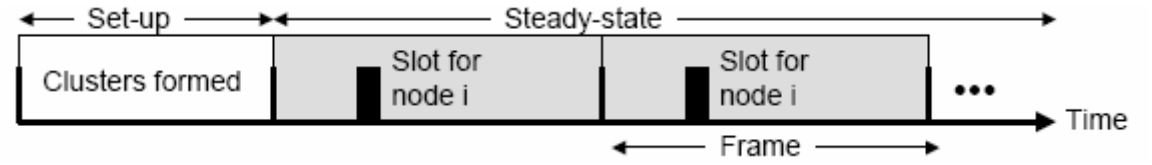

Figure [3.2.2] Time state diagram of steady state 0peration in LEACH protocol

The operation of steady state phase is represented in [1] using the following flow chart diagram.

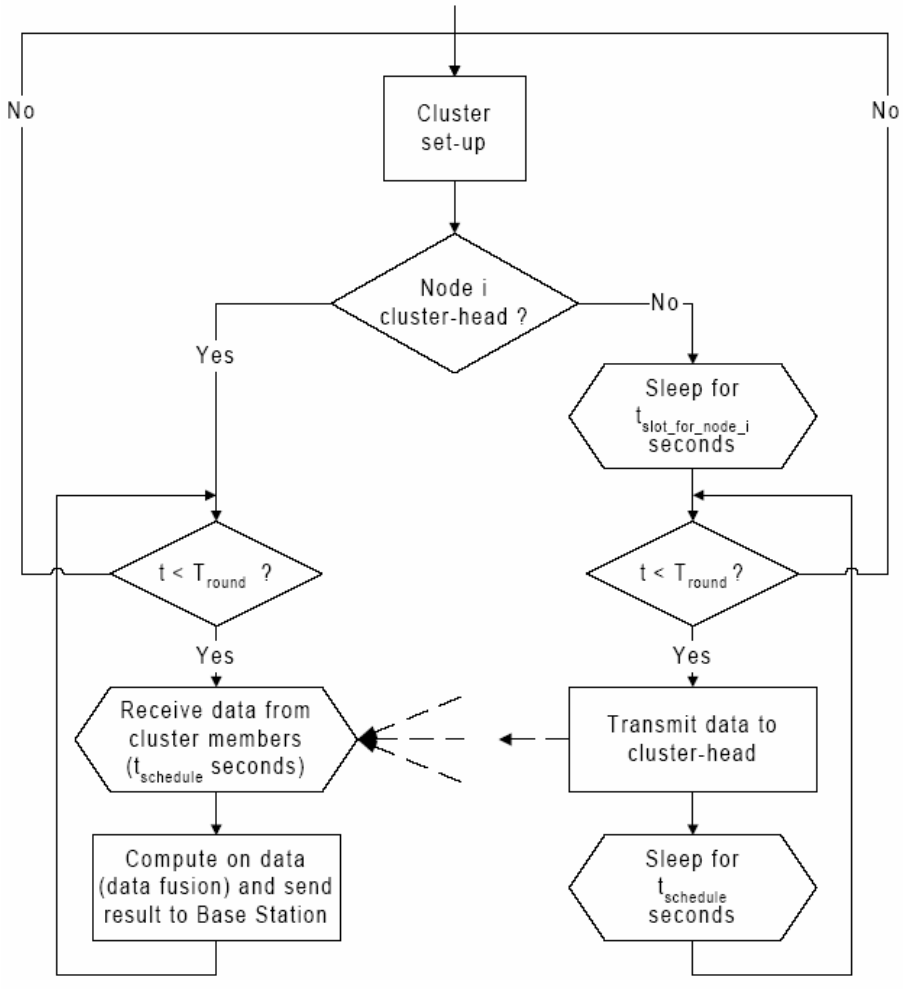

Figure 3.2.1: LEACH Protocol Steady-State Phase

Since the function of this phase is not influenced by the enhancement, this phase is not taken for close analysis in this dissertation.

The total energy spent by a cluster head node, per frame has been derived by the authors of [1] as follows.

$$E_{CH} = lE_{elec}\frac{N}{k} + lE_{BF}\frac{N}{k} + l\epsilon_{two-ray-amp}d_{toBS}^{4} \qquad \text{--- (6)}$$

Where, ECH is the energy spent by the C.H node per frame

l = number of bits in one packet of data
N = the total number of nodes in the network
k = the number of clusters expected to be formed in the network

The energy spent by a non-cluster head node per frame in the steady state phase is give by the equation below

$$E_{non-CH} = lE_{elec} + l\epsilon_{friss\text{-}amp}d^2_{toCH} \quad \text{--- (7)}$$

Where the value of distance d^2_{toCH} has been determined to be calculated by

$$E[d^2_{toCH}] = \frac{1}{2\pi}\frac{M^2}{k} \quad \text{--- (8)}$$

Therefore, substituting the value of distance between the non-cluster head node to the cluster head node in the equation for energy spent by a non cluster head node, has been replaced as

$$E_{non-CH} = lE_{elec} + l\epsilon_{friss-amp}\frac{1}{2\pi}\frac{M^2}{k} \quad \text{--- (9)}$$

CHAPTER 4

ENHANCED ROUTING PROTOCOL FOR GRACEFUL DEGRADATION

4.1 Threshold signal strength for Hello packets

As the cluster head poses to the most vulnerable point available for the intruder to cripple the network with out much effort, the goal of this enhancement is to prevent any adversary from participating in the cluster head selection process. Though encryption is known to pose significant overhead to these poor sensor nodes, our argument is that if encryption is employed only during the setup phase of the network, it is capable of offering the basic first level security. This first level security might not make the network 100% secured, but it is much better than having no security at all. Our aim is to protect this Cluster head position from being taken over by an alien. This would provide only *graceful degradation* in the presence of an adversary, as she is boycotted from taking the more powerful Cluster-Head position.

In LEACH the nodes probabilistically determine if they want to be the next Cluster Head based on the following equation.

$$P_i(t) = \begin{cases} \frac{k}{N - k*(r \bmod \frac{N}{k})} & : \quad C_i(t) = 1 \\ 0 & : \quad C_i(t) = 0 \end{cases} \qquad \text{--- (10)}$$

Where,
k is: number of clusters possible
N is: the total number of nodes in the cluster

If yes they send out a Hello packet with their Node ID and the headers. This packet is encrypted with the public key of that particular node and broadcasted. The receiving nodes first check if the hello packet is encrypted, all un-encrypted packets are discarded.

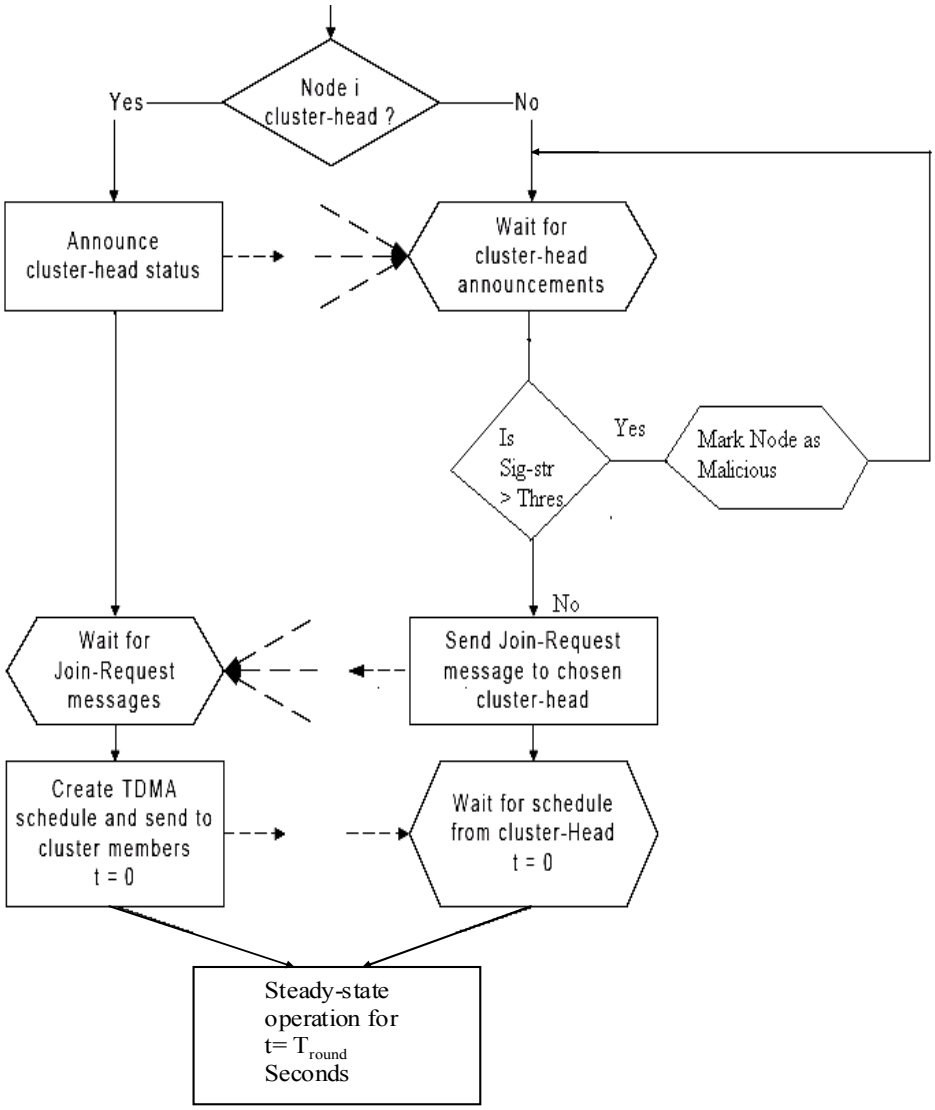

Figure 4.1. The flow chart for the set up phase shown in Figure 3.2.1 is altered with our enhanced mechanism. Threshold signal strength has been assigned in setup phase for the selection of cluster head.

Once the received ADV is found to be an encrypted packet, then the signal strength with which they were received are compared. The Hello packet received with the maximum signal strength but lesser than the set threshold value, is decrypted by the receiving nodes with their own private key.

RC5 Public key mechanism need not necessarily increment the size of the data while encrypting or decrypting it. Therefore, we do not expect any change in the data size due to the introduction of our enhancement mechanism. Ultimately, there is no alteration in the energy spent in the process of transmission and reception. Anyways, there is some energy being spent in the processing stage at the sender's end for encryption and at the receiving node's end for decryption.

A round in LEACH protocol refers to two stages, set-up phase and the steady state phase together. Set-up phase is the stage where clusters are formed and their heads are elected. Once set-up is done, several frames are sent out from the non-cluster head nodes to their head during the steady state phase. The time-line for this operation is as shown in the diagram below.

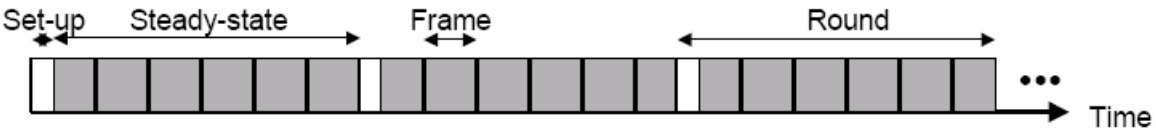

Figure 4.1.1 Time line diagram of LEACH operation

Each round includes a set up phase and a steady state phase which constitutes the transmission of several frames. Of this, our area of focus is only the steady state phase which occupies less than one twelfth of the time taken for one round as represented in the time line diagram above.

The changes encountered by LEACH after our mechanism can be made easy to understand with the following representational diagram.

Considering the criterion that the time spent in the set-up phase is much lesser when compared to that spent in steady state phase, the authors of the LEACH protocol have even neglected the energy spent in the Set-up phase.

While calculating the energy spent per round, only the energy spent in transmitting a frame and the number of frames sent out per round has been considered as seen in the following mathematical model given by the authors of LEACH.

$$E_{cluster} = E_{CH} + \frac{N}{k} E_{non-CH} \qquad \text{--- (13)}$$

This equation denotes that the total energy spent per cluster is equal to the sum of energy spent by the cluster head node and the energy spent by N/k non-cluster head nodes.

In our enhanced protocol we make a correction to the value N/k which is taken as the number of nodes in a cluster. Instead our analysis takes the value of the number of non-cluster head nodes in a cluster as (N/k-1). This is because, the number of nodes in the network is N and the number of clusters is k. Therefore, number of nodes in a cluster including the cluster head is given by N/k. Hence the number of non-cluster head nodes must be taken as (N/k -1) which is number of nodes in a cluster minus the cluster head node.

In LEACH analysis, the energy spent by the radio to transmit an *l*-bit message [1] over a distance d is given by the following equation

$$E_{Tx}(l,d) = \begin{cases} lE_{elec} + l\epsilon_{friss-amp}d^2 & : \quad d < d_{crossover} \\ lE_{elec} + l\epsilon_{two-ray-amp}d^4 & : \quad d \geq d_{crossover} \end{cases} \quad \text{--- (14)}$$

Where, $d_{crossover}$ was considered to be 87 m. In LEACH the distance between the cluster head and the base station is considered to be greater than the cross over distance of 87 m and the distance between the cluster head and the non-cluster head nodes is considered to be lesser than 87m.

4.2 Assumptions:

- We assume that, the sensor network is physically secured. i.e. the physical access to the nodes by any third party has been eradicated. Hence an adversary can physically capture a node to tamper with the burnt in code of a sensor node included in the network
- As the LEACH protocol has been designed for a sensor network where the nodes are stationary, there is no mobility involved in our analysis.
- We also assume that it is not necessary to add any new nodes once the nodes have been dispersed at the venue. If a new set of nodes are to be added, they have to co-ordinate with in themselves and form clusters to operate as a network and cannot interact with the existing nodes as this might bring in lot of complications.
- As the energy spent in encrypting one byte of data is approximately equal

to the energy spent in decrypting the same, we consider the energy spent for encrypting per byte is approximated to energy spent in decrypting per byte of data.

- Likewise, we also assume that the time taken to encrypt a byte of data is approximately equal to the time taken to decrypt the same.
- We engage the Public key cryptography mechanism using RC5 cryptography for encrypting and decrypting the Hello packets broadcasted and the JoinRequest packets, sent in response during the cluster head selection process. Every node in the network is given its public key, a private key and has the list of public keys for all the other nodes that are involved in the network. These keys are burnt in the hardware of the sensor nodes during their manufacturing stage. Hence these keys never have to traverse the channel for any reason.

CHAPTER 5

MATHEMATICAL ANALYSIS

5.1 Math Model:

The two parameters that would experience significant change in their values due to the introduction of encryption and decryption in the operation of LEACH are, increase in the energy consumed and increase in delay.

There is not going to be any increase in the energy spent for the steady state operation because our enhancement technique only aims at protecting the cluster-head post. Hence only the set-up phase is altered which would experience a notable hike in the energy spent. From Ref [1],

$$\text{Energy\_per-round} = \text{Energy\_set-up} + \text{Energy\_steady-state} \quad \text{---- (14)}$$

Based on the analysis discussed by Wendi Heinzelmann [1], as the set-up phase doesn't involve any long distance communication to the Base station or any data processing, the energy spent in this phase is negligent when compared to that consumed in the steady state operation. Thus substituting, $\text{Energy\_set-up} \approx 0$ in equation 1, we get,

$$\text{Energy\_per-round} \approx \text{Energy\_steady-state} \quad \text{--- (15)}$$

Here we derive a mathematical model for considering only this supplementary energy that is expected to be consumed in the process of encryption and decryption of the header of packets traversing the channel during the set-up phase. This is because all the

other steps in the protocol remain unaltered otherwise and the corresponding energy consumption will remain unaffected and need not be calculated for the scope of this dissertation.

5.1.1 Energy Overhead Due to Enhancement

The following math model considers the energy that is expected to be added to the energy spent per round.

Total-Energy-per-round_per-cluster = Energy_setup+Energy_steady-state

+Energy_additional --- (17)

Energy_additional = Energy_encryption_tot + Energy_decryption_tot

= Een-per-bit_at_C.H (no.-of-bits_Hello) (no.-of-nodes_tot) + Ede-per-bit_at_N-C.H (no.-of-bits_Hello) (no.-of-nodes_hearing-Hello) + Een-per-bit_at_N-C.H (no.-of-bits_JReq) (no.-of-nodes_Join-Cluster) +Ede- per-bit_at_C.H (no.-of-bits_JReq) (no.-of-nodes_Join-Cluster)

This can be made simpler as

Energy_additional = e1* B1*N + d2 *B1*n + e2* B2*(n-s) + d1*B2*(n-s) ------ (18)

Where,

e1 = Energy for Encryption-per-bit_at_C.H

e2 = Energy for Encryption-per-bit_at_N-C.H

B1 = Number of bits in Hello Packet

B2 = Number of bits in Join Request

N = Total number of nodes in the network

n = Number of nodes hearing the Hello ADV

s = Number of nodes hearing the Hello but not choosing to join the cluster

(n-s) = Number of nodes sending Join Request to join the cluster

(n-s) can also be represented as (N/k-1) which is nothing but the number of Non-Cluster Head nodes per cluster. Therefore,

$$(n-s) \approx (N/k-1)$$

provided all nodes that send join request to the C.H really join the cluster

Therefore, Eq. 3 becomes

$$\text{Energy\_additional} = e1 * B1*N + d2 * B1*(N/k -1) + e2* B2*(N/k-1) + d1*B2*(N/k-1) \quad \text{--- (19)}$$

Assuming that energy spent per bit for encryption is approximately equal to the energy spent per bit for decryption at both C.H as well as N-C.H nodes we get,

$$e = e1 \approx d1 \text{ and } e = e2 \approx d2$$

Where, e = is the energy spent per bit for encryption/decryption operation. So, equation (19) can be written as

$$\text{Energy\_additional} = e * B1*N+ e*B1*(N/k -1) +e*B2*(N/k -1) +e*B2*(N/k -1) \quad \text{--- (20)}$$

Therefore,

$$\text{Energy\_additional} = e* \{B1* N + B1*n + B2*(N/k) + B2*(N/k) \}$$

As we encrypt only the Hello and Join Request packets exchanged during the set-up phase, we can determine the number of bytes that are expected to be encrypted and

decrypted during this step.

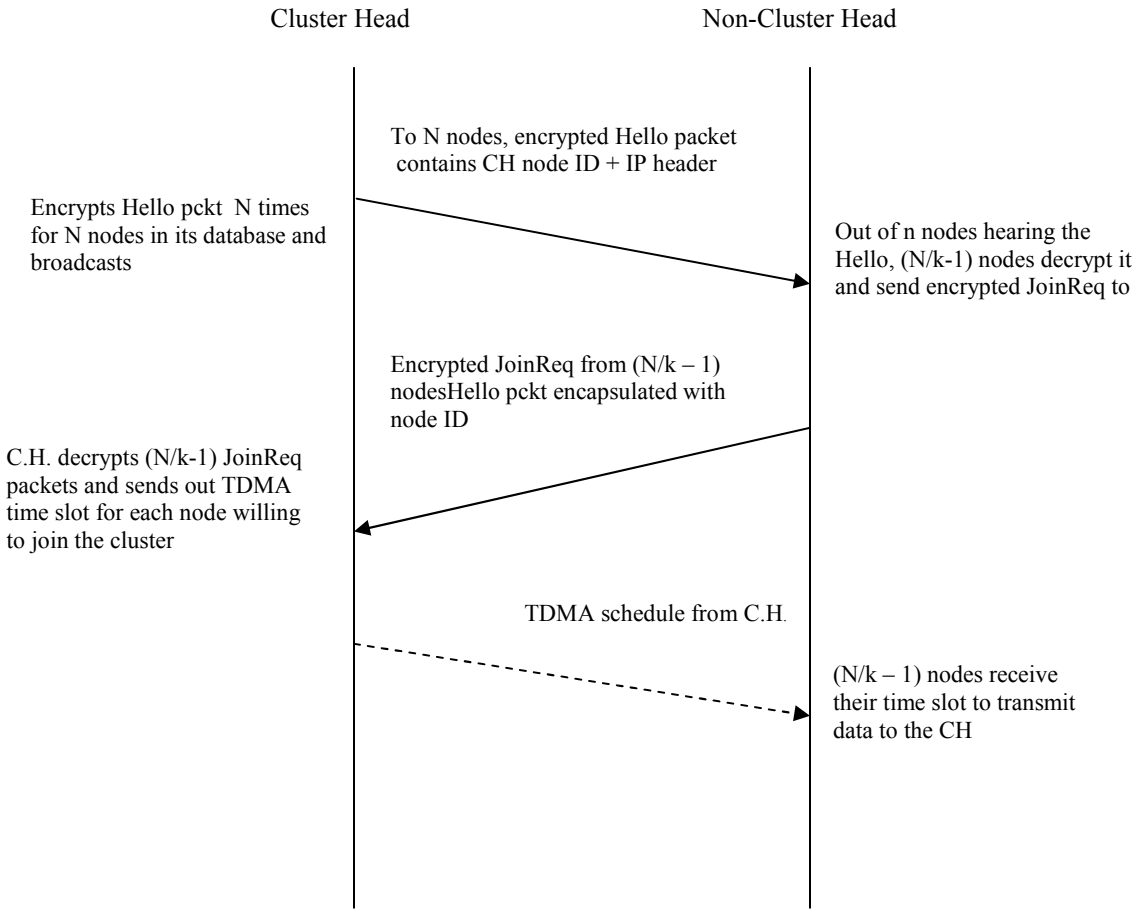

Figure 5.1 Representational diagram of set-up phase in enhanced protocol

Taking the values of the header length in bytes for the Network layer which is 25 Bytes which is given for LEACH's network layer and the Node ID length of value of 6 bytes we can further simplify the above equation as

Header in Bytes for Hello packet = IP Header + Cluster-Head Node ID

= 25 + 6

= 31 Bytes

Header in bytes for Join Request packet is = Hello packet-Header + Node ID

= 31 + 6

= 37 Bytes

Substituting these values in, Eq. 20 and also replacing n by (N/k -1) assuming that all the nodes hearing the ADV decrypt the packet if and only if that packet has reached it with the maximum signal strength but still with in the threshold value set by us when compared to all the Hello packets that reached them in that round. So, as all the nodes decrypting the packet are expected to join the cluster we replace n by (N/k -1) in the following equations. As N/k represents the total number of nodes in a cluster, the number of Non-Cluster heads per cluster is given by (N/k -1),

Energy_additional = e*{31 bytes*N +31 bytes*(N/k -1)+37 bytes* (N/k -1)+37 bytes * (N/K -1)}

= 31 bytes*e*(N+ (N/k -1)) +2*(N/k -1) * e* 37 bytes -----(21)

Multiply equation (21) by the number 8 in order to convert the bytes in to bits, we get

Energy_additional = 8 * e *(31 * (N+ (N/k -1)) + 2* (N/k -1) * 37)

= 8 * e *(31 * (N+ (N/k -1)) + 12* (N/k -1)) * 37) -------(22)

5.1.2 Delay Overhead Due to Enhancement

The overhead imposed over the sensor network in the form of delay is being considered by taking the value calculated in [reference_overhead]. Here the value of time taken to encrypt per bit of data has been calculated considering a sensor node comprising of a StrongARM processor using RC5 methodology for encryption which is the typical scenario of our analysis. Hence, according to this paper, the time taken to encrypt and decrypt for the μamps sensor node has been calculated as 3μs per byte by. This is taken in to consideration for our mathematical model along with the initialization delay of 41μs, every time the decryption/encryption process is performed.

The number of bytes in Hello-packet and the JoinRequest packet has already been calculated as 31 bytes and 38 bytes respectively as shown in section 5.1.1.

Delay_overhead = Time_enc/byte *(Bytes_Hello-packet)* N + Time_dec/byte *(Bytes_Hello-packet)*(N/k -1) + Time_enc/byte * (Bytes_JoinReq) *(N/k -1) + Time_dec/byte*(Bytes_JoinReq) + Init_delay*(N+ 3*(N/k-1)) ---- (23)

As the time for both encryption and decryption has been calculated as 3μs per byte,

Time_enc/byte = Time_dec/byte in Ref [8] by P.Ganesan, R venugopal et al. Hence in the following equation Time_enc/byte and Time_dec/byte can be replace by T = 3μs per byte. The initialization delay has been calculated as 41 μs for every encryption/decryption course which can also be substituted in the place of Init_delay.

Thus, the equation (23) becomes

$$\text{Delay\_overhead} = T*(\text{Bytes\_Hello-packet})*N + T*(\text{Bytes\_Hello-packet})*(N/k-1) + T*(\text{Bytes\_JoinReq})*(N/k-1) + T*(\text{Bytes\_JoinReq}) + \text{Init\_delay}*(N+3*(N/k-1)) \quad \text{--- (24)}$$

$$\text{Delay\_overhead} = T*(31)*N + T*(31)*(N/k-1) + T*(37)*(N/k-1) + \text{Init\_delay}*(N+3*(N/k-1)) \quad \text{---- (25)}$$

Using the math model derived in this chapter the results were simulated using MATLAB. For different values of number of nodes, number of clusters and number of frames per round, the resulting energy spent and delay values were generated and plotted as shown in the next chapter 6.

CHAPTER 6

RESULTS AND ANALYSIS

Using the equation derived for the overhead imposed on a LEACH network in the form of energy and delay are manipulated in this section. Also with the equation derived in [1] for the total energy spent per cluster per round, the total energy spent after enhancement of the LEACH protocol, was compared with the values without enhancement.

The parameters of the experimental conditions taken for simulation using MATLAB are as follows.

The number of nodes in the network N was taken as 100 for the optimal value. For experimental purpose, this value was increased from 100 to 1000 for the same conditions as used to simulate LEACH. Hence we could analyze and compare the variation in the energy spent and delay overhead of our enhanced protocol versus LEACH.

The values for the energy overhead, delay over head were calculated and plotted against the number of clusters k and also against the Number of frames sent out per round keeping the number of nodes in the network N constant.

6.1. a. Energy additional due to enhancement of LEACH

The following graph shows the plot of energy overhead per round, per cluster, due to the proposed enhancement to LEACH, the total energy spent per cluster per round in LEACH without enhancement, and the final energy which is the sum of the energy generally spent in LEACH mechanism plus the additional energy that would be spent in

order to bring in graceful degradation in the network performance during attempts to invasion. All these three values are plotted by assigning different values for the number of clusters in the network k.

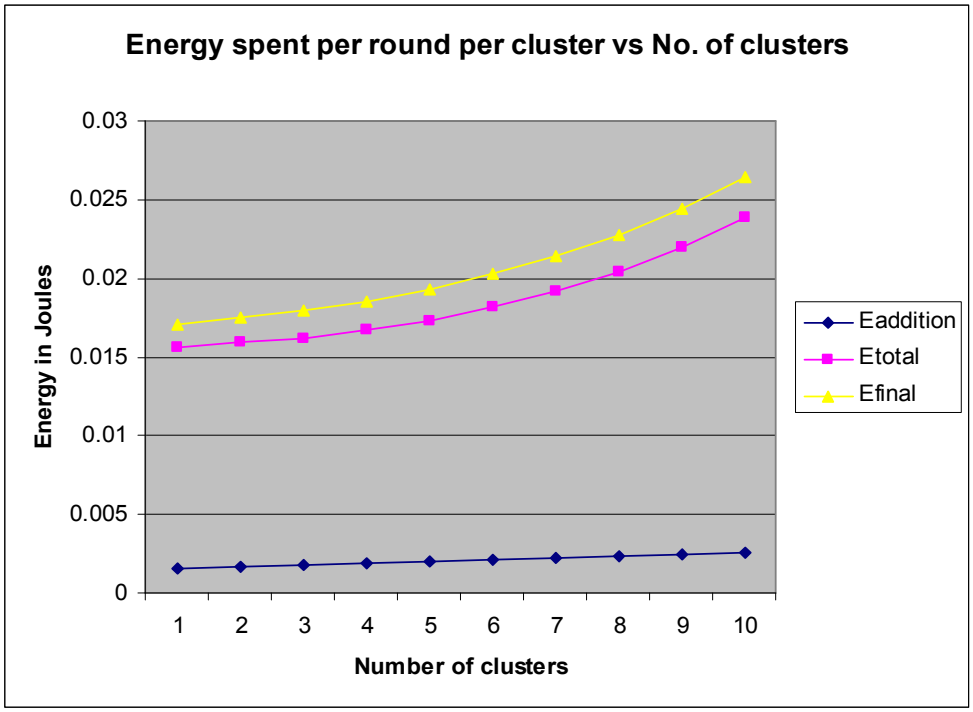

Figure 6.1 Graph A.. Energy spent per round per cluster vs. Number possible of clusters in the network. k value is varied from 1 to 10 with the total number of nodes in the network N is kept constant as 100.

- Eaddition is the energy that is expected to get added to the total energy spent per cluster per round in LEACH.
- Etotal is the total energy spent in LEACH per cluster per round.
- Efinal is the sum of Eaddition and Etotal.

The values of energy spent are in micro Joules. The number of clusters is varied from 1 where the whole network forms into one single cluster, to 10 where the network consists of 10 clusters.

From the Graph A shown in Figure 6.1 it is evident that the Eaddition varies very slightly with the increase in number of clusters as Eaddition is a factor confined to the setup phase which is a very small portion of a round as shown in section 4.1. The authors of LEACH have even eliminated the energy spent for setup phase as it is very small, when compared to the energy expend in the steady state operation.

Analyzing Graph A we could conclude that with this very small increase in the energy spent per round we can prevent any malicious node from participating in the cluster head election process and compete for the cluster head position. By spending Efinal with is little bit more than the energy spent in LEACH we can avoid sink hole attacks and Hello flood attacks in the wireless sensor network.

6.1. b. Final energy spent in Enhanced LEACH's set-up phase and hence the cluster head position

The following graph, Graph2 represents the variation in the final energy spent in the Enhanced LEACH for different values of number of frames sent per round in the steady state phase.

The final energy spent per round per cluster increases as the total number of nodes in the cluster is increased keeping all the other parameters constant. This is because with the increase in the number of nodes, the number of nodes per cluster increases which in turn results in the increase of number of packets sent out and received during both the setup phase and the steady state phase.

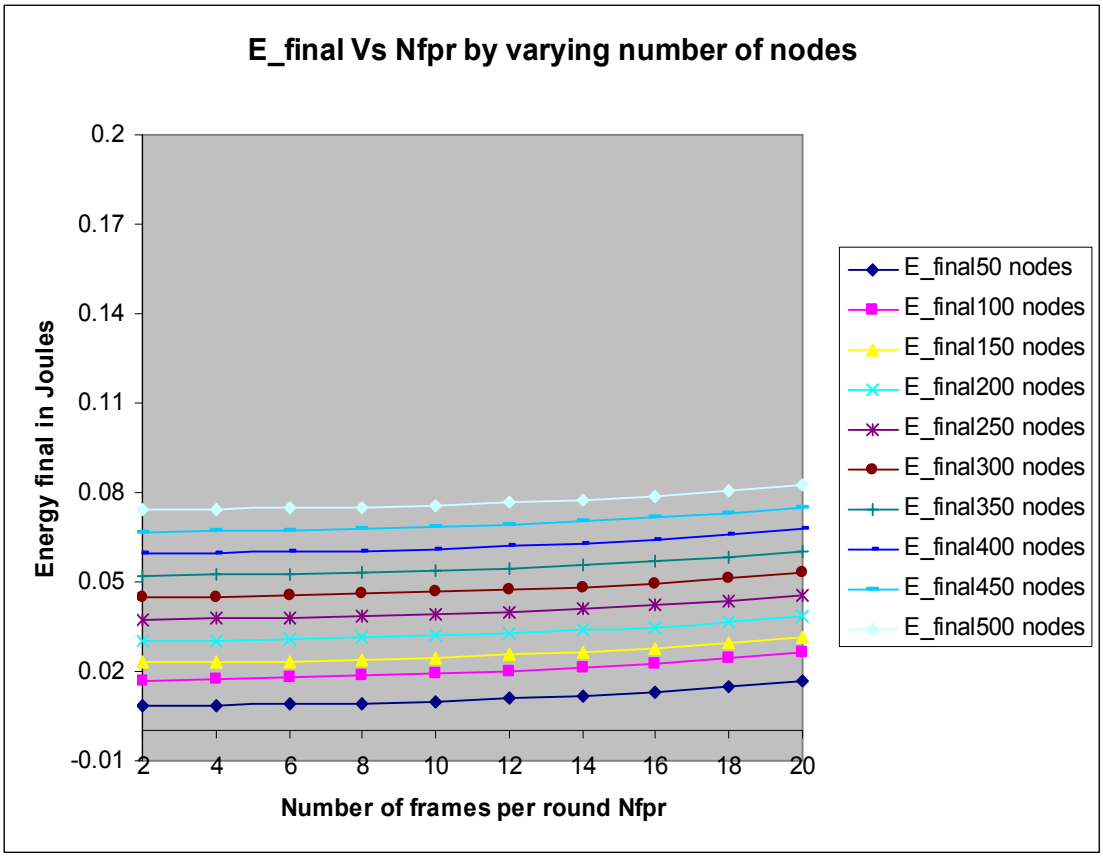

Figure 6.2 Graph 2. Energy final vs. No. of frames per round for different number of nodes in the network N.

6.2 Delay Overhead

Delay overhead is the delay added at various steps of setup phase in LEACH due to encryption and decryption taking place at the cluster head and non-cluster head nodes. This is calculated by taking the value for the time taken to encrypt and decrypt per bit of data in the [8] which are equal to 3μs. The delay over head mainly depends on the total number of nodes.

6.2.1 Variation in delay overhead as the number of clusters in the network is varied

The following graph 3 shows the plot of delay overhead due to enhancement of leach against the number of possible clusters expected in the network.

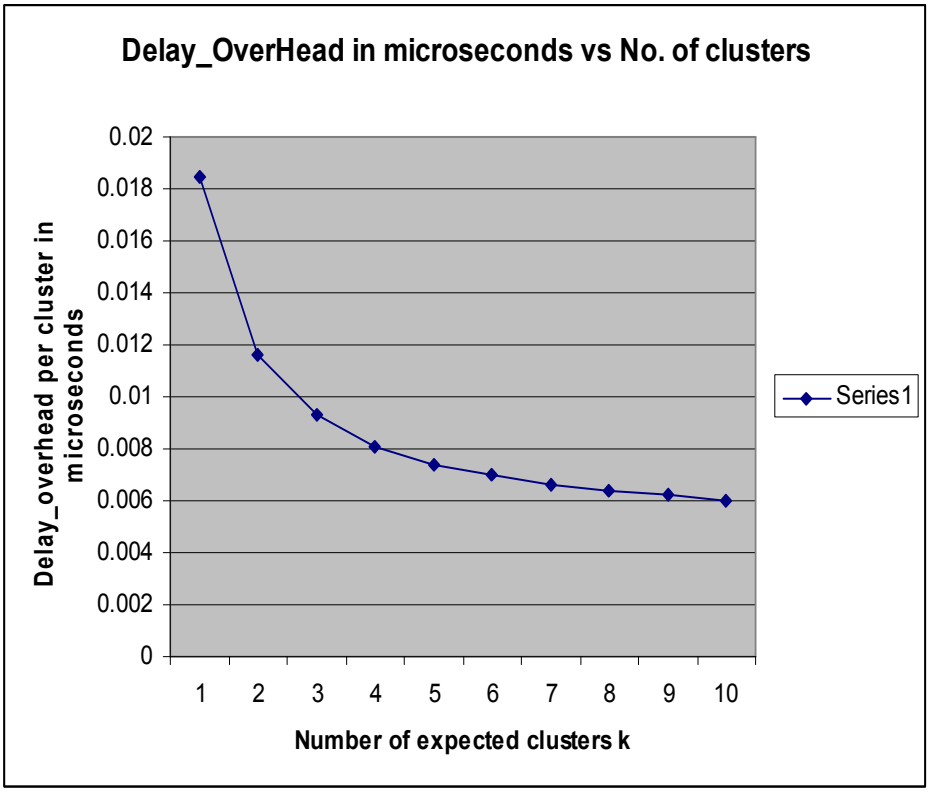

Figure 6.3 Graph 3. Delay overhead in micro seconds encountered by enhanced LEACH plotted against the number of clusters k

As shown in the graph the delay due to encryption and decryption of the Hello and the Join Request packets in the setup phase decrease steeply with the increase in the number of clusters in the network. This is mainly due to the fact that with the increase in the number of clusters k while the number of nodes in the network N is kept as a constant

100, the number of nodes per cluster (N/k) decreases. Hence the number of Hello packets and Join Request packets traversing in the setup phase also decrease, leading to the reduction in time taken for the process of encryption and decryption per cluster.

6.2.2 Delay overhead as the number of nodes in the network for the same experimental parameters is increased

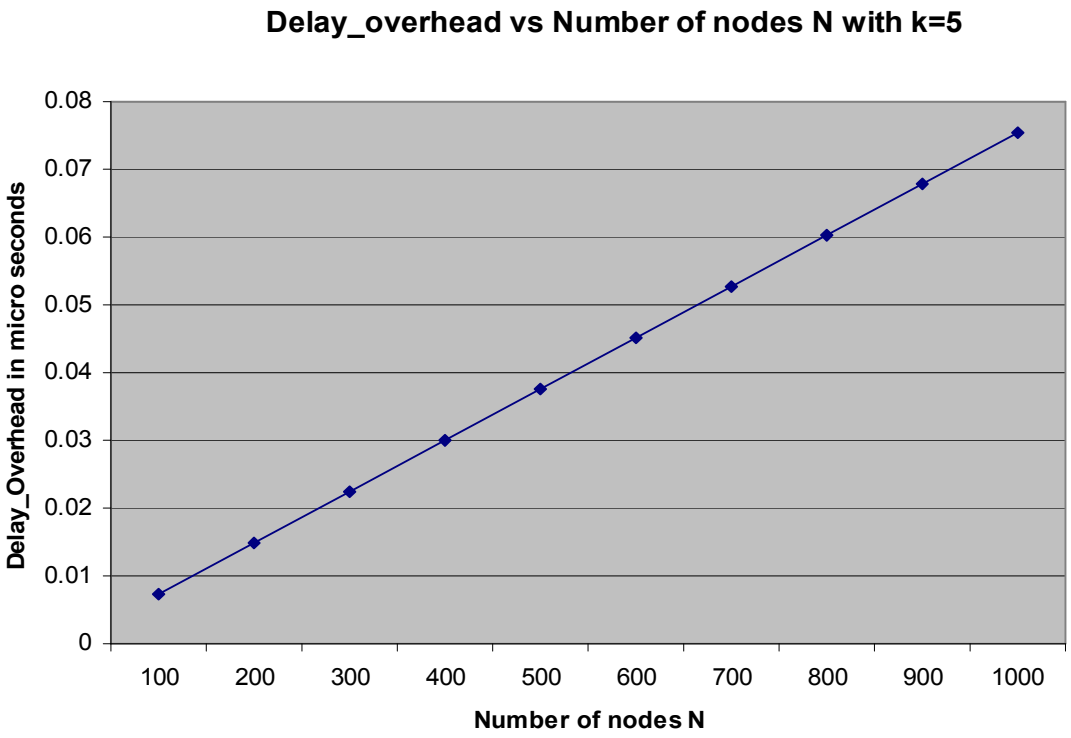

Figure 6.4 Graph 4. Delay overhead varying with the increase in the total number of nodes in the network keeping all other parameters constant.

From the above graph, we observe that the delay overhead is constantly increasing with the number of nodes in the network. This is due to the increase in the number of nodes per cluster, keeping the number of clusters k constant. Hence the time taken for encrypting also increases. Number of decryptions in the setup phase also rises due to increased number of Hello packets and Join Request packets sent out in this phase.

CHAPTER 7

CONCLUSION AND FUTUREWORK

From the math model derived and discussed in Chapter 6 it is determined that the energy spent due to the introduction of a basic level of security is very less when compared to the total energy spent during the general operation of the LEACH protocol. By securing the Cluster Head post from being occupied by malicious node we can avoid Hello attacks, sink-hole attacks and worm-hole attacks. As we also set up a threshold value for the Hello packet signal strength, we restrict the effect of a laptop class adversary's superiority. Hence a drastic, instantaneous attack is avoided and invasion can only degrade the network performance gracefully.

An analytical model was derived for the additional energy spent per round for encryption/decryption operations. The mathematical equation for calculating the delay encountered in the set-up phase due to the introduction of encryption and decryption in the protocol is shown in Eq. 25. The delay values were found to me in the order of $1/1000^{th}$ of a micro second which is negligible when compared to 25 μseconds of transmission delay encountered in the LEACH protocol.

This enhanced protocol for graceful degradation of wireless sensor network only provides solutions for the LEACH protocol. Research can be done to achieve same enhancement on other clustering protocols, as all decentralized clustering protocols are exposed to similar attacks like Hello flood attack, worm-hole attack and sink-hole attack.

LIST OF REFERENCES

LIST OF REFERENCES

[1] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," 33rd Annual Hawaii International Conference on System Sciences, 2000, Pages: 3005–3014

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and counter measures," Elsevier's AdHoc Networks Journal, Volume.1, Issue: 2-3, Pages: 293-315, September 2003

[3] A. Akyildiz, *et al*, "A Survey on Sensor Networks", Communications Magazine, IEEE, Volume: 40, Issue: 8, Aug. 2002 Page(s): 102 –114

[4] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, "*A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols*", In Proceedings of the ACM International Conference on Mobile Computing and Networking, Mobicom

[5] N.Xu, "A Survey on Sensor Network Application" Processing, vol. 14, no. 7, pp. 849–991, July 2005

[6] C. Perkins and P. Bhagwat, "*Highly Dynamic Destination-Sequenced Distance-Vector Routing DSDV_for Mobile Computers*". In Proceedings of the SIGCOMM - Conference on Communications Architectures, Protocols and Applications

[7] C. Perkins and E. Royer, "*Ad-Hoc On_Demand Distance Vector AODV-Routing*", In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications , WMCSA

[8] P.Ganesan, R.Venugopalan, P. Peddabachagari, A.Dean, F.Mueller, M.Sichitiu, "*Analyzing and Modeling Encryption Overhead for Sensor Network Nodes"* International Workshop on Wireless Sensor Networks and Applications Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications

[9] http://security.ece.orst.edu/koc/ece575/97Project/Sadagopan+Shah/sld001.html "RC5 encryption algorithm"

[10] G.Gaubatz, J.P.Kaps, B.Sunar, "*Public Key Cryptography in Sensor Networks|Revisited *".* In ESAS, pages 2-18, 2004

[11]. K, Scott and N, Bambos, "*The Self_Organizing Wireless Adaptive Network (SWAN) Protocol for Communication Among Mobile Users*". In Proceedings of the IEEE Globecom

[12]. T. Meng and R, Volkan, "*Distributed Network Protocols for Wireless Communication"* In Proceedings of IEEEE ISCA

[13] S. Park and M. Srivastava. "*Power Aware Routing in Sensor Networks using Dynamic Source Routing*", In ACM MONET Special Issue on Energy Conserving Protocols in Wireless Networks