Analysis of Low Energy Adaptive Clustering Hierarchy (LEACH) protocol

A thesis submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology

in

Computer Science and Engineering

by

Taran Deep Singh Pawa

(Roll no. 107CS007)

Under the guidance of :

Prof. S.K.Jena

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela-769 008, Orissa, India

National Institute of Technology Rourkela

Certificate

This is to certify that the project entitled, '**Analysis of Low Energy Adaptive Clustering Hierarchy (LEACH) protocol**' submitted by **Taran Deep Singh Pawa** is an authentic work carried out by them under my supervision and guidance for the partial fulfillment of the requirements for the award of **Bachelor of Technology Degree** in **Computer Science and Engineering** at **National Institute of Technology, Rourkela**.

To the best of my knowledge, the matter embodied in the project has not been submitted to any other University / Institute for the award of any Degree or Diploma.

Date - 09/05/2011
Rourkela

(Prof. S.K.Jena)
Department of Computer Science and Engineering

Acknowledgments

I express my profound gratitude and indebtedness to **Prof. S.K.Jena**, Department of Computer Science and Engineering, NIT, Rourkela for introducing the present topic and for his inspiring intellectual guidance, constructive criticism and valuable suggestion throughout the project work.

I am also thankful to **Mr. Suraj Sharma**, Department of Computer Science and Engineering for motivating me throughout the project.

Finally, I would like to thank my parents for their support and motivation to complete this project.

Date - 09/05/2011
Rourkela

Taran Deep Singh Pawa

Abstract

Sensor network consists of tiny sensors and actuators with general purpose computing elements to cooperatively monitor physical or environmental conditions, such as temperature, pressure, etc. Wireless Sensor Networks are uniquely characterized by properties like limited power they can harvest or store, dynamic network topology, large scale of deployment. Sensor networks have a huge application in fields which includes habitat monitoring, object tracking, fire detection, land slide detection and traffic monitoring. Based on the network topology, routing protocols in sensor networks can be classified as flat-based routing, hierarchical-based routing and location-based routing. These protocols are quite simple and hence are very susceptible to attacks like Sinkhole attack, Selective forwarding, Sybil attack, Wormholes, HELLO flood attack, Acknowledgement spoofing or altering, replaying routing information. Low Energy Adaptive Clustering Hierarchy (LEACH) is an energy-efficient hierarchical-based routing protocol. Our prime focus was on the analysis of LEACH based upon certain parameters like network lifetime, stability period, etc. and also the effect of selective forwarding attack and degree of heterogeneity on LEACH protocol. After a number of simulations, it was found that the stability regions length is considerably increased by choosing an optimal value of heterogeneity; energy is not properly utilized and throughput is decreased in networks compromised by selective forwarding attack but the number of cluster-heads per round remains unaffected in such networks.

Contents

List of Figures

1 INTRODUCTION

1.1 INTRODUCTION

Like living organisms, a variety of modern devices and equipments relies on the sensory data from the real world around it. These sensory data comes is provided by Wireless Sensor Networks (WSN), which consists of several tiny sensor nodes to monitor physical or environmental conditions, such as temperature, vibration, pressure, sound or motion, and then collectively send these information to a central computing system, called the base station or sink. Different routing protocols govern the movement of this information. Broadly the routing protocols can be classified as flat-based routing, hierarchical-based routing, and location-based routing. LEACH (Low Energy Adaptive Clustering Hierarchy) is a hierarchical-based routing protocol which uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. Sensor network protocols are quite simple and hence are very susceptible to attacks like Sinkhole attack, Selective forwarding, Sybil attack, Wormholes, HELLO flood attack, Acknowledgement spoofing, altering, replaying routing information. For example, Selective forwarding and HELLO flood attack affects networks with clustering based protocols like LEACH.

1.2 MOTIVATION

Wireless Sensor Networks (WSN) is an active research area in todays computer science and telecommunication. The development of clustered sensor networks have recently been shown to decrease system delay, save energy while performing data aggregation and increase system throughput. These are strong motivational points behind selecting LEACH as the baseline protocol for the analytical study. Also LEACH has a few but very significant disadvantages like it assumes all the nodes to have same energy, which is not the case always in real-time problems, its cannot be applied for mobile nodes, failure of cluster-heads creates a lot of problems and it doesnt take into account that the systems might have multiple base stations.

1.3 OBJECTIVE

This thesis gives a detailed simulation study of the LEACH protocol and the effect of selective forwarding attack on it. The parameters considered for the analytical study are the network lifetime, the throughput, the stability period, the instability period of the network and the field distribution. Also the effect of heterogeneity in the network is focused during the simulations.

2 BACKGROUND

2.1 WIRELESS SENSOR NETWORK

Sensor networks refers to a heterogeneous system consisting of multiple detection stations called sensor nodes with a communications infrastructure intended to monitor and record conditions at diverse locations. Sensor nodes, also known as mote, are small, lightweight and portable devices equipped with a transducer, microcomputer, transceiver, and power source. The transducer produces electrical signals based on the sensed physical phenomena. The microcomputer processes and stores the sensed information. The transceiver receives instructions from the base station/central computing system and sends data to it. Each sensor nodes derives its energy usually from a battery or any other embedded form of energy harvesting. The size of the sensor nodes vary from that of a shoebox to that of a minute sand-particle. Similarly their cost also varies from hundreds of dollars to a few pennies. Size and cost constraints result in corresponding constraints on energy, memory, computational speed and communications bandwidth.
Wireless Sensor Networks are characterized by :

- Limited power they can harvest or store
- Ability to cope with node failures
- Heterogeneity of nodes
- Large scale of deployment
- Mobility of nodes
- Communication failures
- Dynamic network topology
- Ability to withstand harsh environmental conditions

2.2 APPLICATION OF WIRELESS SENSOR NETWORK

Wireless Sensor Networks (WSN) offers a rich, multi-disciplinary area of research, in which a number of tools and concepts can be applied to address a whole diverse set of applications. Sensor networks may consist of many dierent types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of conditions. These sensor nodes can be put for continuous sensing, location sensing, motion sensing and event detection. The idea of micro-sensing and wireless connection of these sensor nodes promises many new application areas. A few examples of their applications are as follows:

2.2.1 AREA MONITORING APPLICATIONS

Area monitoring is a very common application of WSNs. In area monitoring, the WSN is deployed over a region where some physical activity or phenomenon is to be monitored. When the sensors detect the event being monitored (sound, vibration), the event is reported to the base station, which then takes appropriate action (e.g., send a message on the internet or to a satellite). Similarly, wireless sensor networks can be deployed in security systems to detect motion of the unwanted, traffic control system to detect the presence of high-speed vehicles. Also WSNs finds huge application in military area for battleeld surveillance, monitoring friendly forces, equipment and ammunition, reconnaissance of opposing forces and terrain, targeting and battle damage assessment.

2.2.2 ENVIRONMENTAL APPLICATIONS

A few environmental applications of sensor networks include forest fire detection, greenhouse monitoring, landslide detection, air pollution detection and flood detection. They can also be used for tracking the movement of insects, birds and small animals, planetary exploration, monitoring conditions that affect crops and livestock and facilitating irrigation.

2.2.3 HEALTH APPLICATIONS

Some of the health applications for sensor networks are providing interfaces for the disabled, integrated patient monitoring, diagnostics, drug administration in hospitals, monitoring the movements and internal processes of insects or other small animals, telemonitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.

2.2.4 INDUSTRIAL APPLICATIONS

WSNs are now widely used in industries, for example in machinery condition-based maintenance. Previously inaccessible locations, rotating machinery, hazardous or restricted areas, and mobile assets can now be reached with wireless sensors.
They can also be used to measure and monitor the water levels within all ground wells and monitor leachate accumulation and removal.

2.2.5 OTHER APPLICATIONS

Sensor networks now find huge application in our day-to-day appliances like vacuum cleaners, micro-wave ovens, VCRs and refrigerators. Other commercial applications includes constructing smart oce spaces, monitoring product quality, managing inventory, factory instrumentation and many more.

2.3 ROUTING PROTOCOLS

[2] Depending upon the network structure, routing in wireless sensor networks can be classified as flat-based routing, hierarchical-based routing, and location-based routing.

- In flat-based routing, all the nodes in the topology are assigned the same functionality or role.
- In hierarchical-based routing, nodes are assigned different roles or functionalities according to the hierarchy.

- In location-based routing, routing path for the data is decided according to the sensor nodes position in the field.

Depending on how the source finds a route to the destination, routing protocols can be classified into three categories, namely, proactive, reactive, and hybrid protocols.

- In proactive protocols, all routes are computed before they are actually needed.
- In reactive protocols, routes are computed only when they are needed.
- While hybrid protocols are combination of the above two ideas.

Depending on the protocol operation, routing protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing.

- In multipath-based routing, multiple paths are used to enhance network performance i.e. fault tolerance, balance energy consumption, energy-efficiency and reliability.
- In query-based routing, destination nodes propagate a query for data. Usually these queries are described in natural language or high-level query language.
- In negotiation-based routing, high-level data descriptors are used in order to eliminate redundant data transmissions through negotiation. Communication decisions are also made based on the resources available to them.
- In QoS-based routing, a balance between energy consumption and data quality is maintained.
- In coherent-based routing, the data is aggregated with minimum processing before forwarding. Here, energy efficiency is achieved by path optimality.

Apart from these protocols, a number of protocols exist that depend upon timing and position information.

2.4 ATTACKS ON ROUTING PROTOCOL

Since the sensor network protocols are quite simple, they are susceptible to a number of network layer attacks. A few of these attacks [12] are:

- Spoofed, altered, or replayed information
- Selective forwarding
- Sinkhole attack
- HELLO flood attack
- Sybil attack
- Wormholes

2.4.1 SPOOFED, ALTERED, OR REPLAYED INFORMATION

The most direct and most effective way of attacking any routing protocol is to target the information being exchanged between the nodes. By spoofing, altering or replaying routing information, adversaries can achieve a number of motives like creating routing loops, extending or shortening routing paths, attracting or repelling network traffic, increasing end-to-end latency, partitioning the network, generating false error messages, etc.

2.4.2 SELECTIVE FORWARDING

An honest node would always faithfully forward received messages to its destination. However, a malicious node would refuse to forward certain messages and simply drop them, ensuring that the message doesnt reach the intended destination. This is called selective forwarding attack. A simple form of this attack is that the malicious node would act as a black-hole i.e. drops every message packet that arrives to it. But such nodes have the risk that the neighboring nodes would consider them as dead nodes and would seek another route. So, adversaries adapt a more subtle form i.e. intelligently forward only certain messages. Hence, the risk of getting caught is minimized.
Selective forwarding attacks are more effective when the attacker explicitly includes itself

in the routing path of the data. Other ways of implementing selective forwarding is by jamming or causing collision on the transmitting information.

2.4.3 SINKHOLE ATTACK

In sinkhole attack, a compromised node is made to look very attractive to the surrounding nodes with respect to the routing algorithm. (For example, adversary can advertise a very high quality routing path and hence divert the path through it.)Hence a metaphorical sinkhole is created with the adversary at the center. And now since the routing path is diverted through this adversary node, severe damages can be done by it. Sinkhole is a very effective way of implementing selective forwarding. Spoofing, altering or replaying the routing information can also be done by the adversary.

The reason why sensor networks are highly susceptible to sinkhole attack is because all message packets being transmitted have a single ultimate destination, the base station. A compromised node only needs to provide a single high quality route to the base station and hence, effecting severe damages.

2.4.4 HELLO FLOOD ATTACK

Many protocols require broadcasting HELLO packets by the sensor nodes to announce it to the neighbors, thereby alerting them that its within their transmission range. But an adversary could flood false HELLO packets. Hence, the nodes would consider it to be within the range while the adversary may be situated far from it. In such scenarios, nodes would be unnecessarily transmitting message and hence draining its energy. Protocols which depend upon exchange of location information between the nodes are likely to be targets of such attack.

2.4.5 SYBIL ATTACK

In Sybil attack, a single node presents multiple identities to the other nodes in the network. Routes believed to be passing through multiple nodes would actually be passing through the same adversary node and hence thereby running the risk of an endless loop. Sybil stack pose significant threats to location-based routing protocol. Protocols which

require exchange of location information would be adversely affected as adversary nodes, using Sybil attack, would be exchanging multiple sets of coordinates, rather than a single set of coordinates and hence can be in more than one place at a time.

2.4.6 WORMHOLES

In wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different path. Wormhole attack normally involves two distant malicious nodes, misleading others to understate the distance between them by relaying packets along an outer channel, which is available only to the attacker. An attacker situated close to the base-station may completely disrupt the routing by creating a well-placed wormhole. This attack is likely to be used in combination with eavesdropping or selective forwarding. Detecting Wormhole attack is difficult when used along with Sybil attack. Wormholes can be intelligently used to create sinkholes.

3 LEACH

3.1 INTRODUCTION

Heinzelman, et.al [5] introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH arranges the nodes in the network into small clusters and chooses one of them as the cluster-head. Node first senses its target and then sends the relevant information to its cluster-head. Then the cluster head aggregates and compresses the information received from all the nodes and sends it to the base station. The nodes chosen as the cluster head drain out more energy as compared to the other nodes as it is required to send data to the base station which may be far located. Hence LEACH uses random rotation of the nodes required to be the cluster-heads to evenly distribute energy consumption in the network. After a number of simulations by the author, it was found that only 5% of the total number of nodes needs to act as the cluster-heads. TDMA/CDMA MAC is used to reduce inter-cluster and intra-cluster collisions. This protocol is used were a constant monitoring by the sensor nodes are required as data collection is centralized (at the base station) and is performed periodically.

3.2 OPERATION

LEACH operations can be divided into two phases:-

1. Setup phase
2. Steady phase

In the setup phase, the clusters are formed and a cluster-head (CH) is chosen for each cluster. While in the steady phase, data is sensed and sent to the central base station. The steady phase is longer than the setup phase. This is done in order to minimize the overhead cost.

1. Setup phase :- During the setup phase, a predetermined fraction of nodes, p, choose themselves as cluster-heads. This is done according to a threshold value, T(n). The

threshold value depends upon the desired percentage to become a cluster-head- p, the current round r, and the set of nodes that have not become the cluster-head in the last 1/p rounds, which is denoted by G. The formulae is as follows :

$$T(n) = \frac{p}{1-p\times(r\times mod\frac{1}{p})} \; \forall n \in G$$

Every node wanting to be the cluster-head chooses a value, between 0 and 1. If this random number is less than the threshold value, T(n), then the node becomes the cluster-head for the current round. Then each elected CH broadcasts an advertisement message to the rest of the nodes in the network to invite them to join their clusters. Based upon the strength of the advertisement signal, the non-cluster head nodes decide to join the clusters. The non-cluster head nodes then informs their respective cluster-heads that they will be under their cluster by sending an acknowledgement message. After receiving the acknowledgement message, depending upon the number of nodes under their cluster and the type of information required by the system (in which the WSN is setup), the cluster-heads creates a TDMA schedule and assigns each node a time slot in which it can transmit the sensed data. The TDMA schedule is broadcasted to all the cluster-members. If the size of any cluster becomes too large, the cluster-head may choose another cluster-head for its cluster. The cluster-head chosen for the current round cannot again become the cluster-head until all the other nodes in the network havent become the cluste-head.

2. Steady phase :-During the steady phase, the sensor nodes i.e. the non-cluster head nodes starts sensing data and sends it to their cluster-head according to the TDMA schedule. The cluster-head node, after receiving data from all the member nodes, aggregates it and then sends it to the base-station

After a certain time, which is determined a priori, the network again goes back into the setup phase and new cluster-heads are chosen. Each cluster communicates using different CDMA codes in order to reduce interference from nodes belonging to other clusters.

3.3 ATTACKS

LEACH protocol is difficult to attack as compared to the more conventional multi-hop protocols. In the conventional multi-hop protocols, the nodes around the base station are more attractive to compromise. Whereas in LEACH, the CHs are the only node that directly communicate with the base station. The location of these CHs can be anywhere in the network irrespective of the base station. And more over the CHs are periodically randomly changed. So spotting these CHs is very difficult for the adversary.

However, because it is a cluster-based protocol, relying fundamentally on the CHs for data aggregation and routing, attacks involving CHs are the most damaging. If any adversary nodes become a CH, then it can facilitate attacks like Sybil attack, HELLO flood attack and selective forwarding. The intruder can broadcast a powerful advertisement to all the nodes in the network and hence, every node is likely to choose the adversary as the cluster-head. The adversary can then selectively forward information to the base-station or modify or dump it.

Key management is an effective method to improve network security. These schemes typically assume that a node interacts with a quite static set of neighbors and that most of its neighborhood is discovered right after the deployment. However, clusters in LEACH are formed dynamically (at random) and periodically, which changes interactions among the nodes and requires that any node needs to be ready to join any CH at any time. There are a number of standard key distribution schemes but most of them are ill suited to WSNs: for example, public key based distribution requires a lot of processing; global keying is quite vulnerable; and, complete pairwise keying requires a huge memory [13]. And since WSNs consists of sensors with small computational power and negligible memory they are unable to incorporate these security mechanisms.

3.4 ASSUMPTIONS

LEACH protocol takes into a number of assumptions which may create a lot of problems in the real-time systems. A few of these assumptions are as follows:

- All nodes can transmit with enough power to reach the base station if needed.

- Each node has computational power to support different MAC protocols.
- Nodes always have data to send.
- Nodes located close to each other have correlated data.
- All nodes begin with the same amount of energy capacity in each election round, assuming that being a CH consumes approximately the same amount of energy for each node.

3.5 VARIATIONS

3.5.1 F-LEACH

L. B. Oliveria et al.[9] propoesed FLEACH, a protocol for securing node to node communication in LEACH-based network. It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. FLEACH provides authenticity, integrity, condentiality and freshness to node-to-node communication. But it is valnera- ble to node capturing attack.

3.5.2 SLEACH

This is the first modied secure version of LEACH called SLEACH [1], which investigated the problem of adding security to cluster-based communication protocol for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources. SLEACH provides security in LEACH by using the building block of SPINS (Security Protocol for Sensor Network), symmetric-key methods and MAC (Message Authentication Code). SLEACH protects against selective forwarding, sinkhole and HELLO ooding attacks. It prevents intruder to send bogus sensor data to the CH and CH to forward bogus message. But SLEACH cannot prevent to crowd the time slot schedule of a cluster, causing DoS at- tack or simply lowering the throughput of the CH and does not guarantee data condentiality. The solution is meant to protect only outsider attack.

3.5.3 R.Srinath et al.

This protocol is based on LEACH protocol; named Authentication Condentiality cluster based secure routing pro- tocol [10]. It uses both public key (in digital signature) and private key cryptography. This protocol deals with interior adversary or compromised node. Because of the high com- putational requirement (use of public key cryptography), it is not ecient for the WSNs.

3.5.4 NHRPA

The proposed routing protocol [3] can adopt suitable routing technology for the nodes according to the distance of node to the BS, density of the nodes distribution and residual energy of the nodes. NHRPA compared with Directed Diusion (DD), LEACH and PEGASIS in terms of the energy usage, packet latency and security in the presence of node compromised attacks, results show that the proposed routing algorithm is more ecient for WSNs. It does not use any cryptography technique in the routing protocol, so the overhead is less. But it only deals with the node compromise attack.

3.5.5 Sec-LEACH

Sec-LEACH [8] provides an ecient solution for securing communications in LEACH. It used random-key pre-distribution and TESLA for secure hierarchical WSN with dynamic cluster formation. Sec-LEACH applied random key distribution to LEACH, and introduced symmetric key and one way hash chain to provide condentiality and freshness. Sec-LEACH provides authenticity, integrity, condentiality and freshness to communications

3.5.6 SS-LEACH

Di Wu et al.[4] introduced a secure hierarchical protocol called SS-LEACH, which is the secure version of LEACH. SS- LEACH improves the method of electing cluster heads and forms dynamic stochastic multi-paths cluster heads chains to communicate to the base station, In this way it improve the energy-eciency and hence prolong the lifetime of the

network. It used the key pre-distribution and self-localization technique to secure the basic LEACH protocol. It prevent compromised node to take part in the network and preserve the secrecy of the packet. It avoids selective forwarding, HELLO ooding and Sybil attack.

3.5.7 RLEACH

Secure solution for LEACH has been introduced called RLEACH [7] in which cluster are formed dynamically and periodically. In RLEACH the orphan node problem is raised due to random pair-wise key scheme so they have used improved random pair-wise key scheme to overcome. RLEACH has been used the one way hash chain, symmetric and asymmetric cryptography to provide security in the LEACH Hi- erarchical routing protocol. RLEACH resists to many attack like spoofed, alter and replayed information, sinkhole, worm- hole, selective forwarding, HELLO ooding and Sybil attack.

3.5.8 ESMR

Proposed model is the security solution for the LEACH called ecient security model of routing protocol (ESMR)[6], which use only public key cryptography technique. Simulation result shows that the performance of ESMR is not as good as LEACH in no attacker environment, but it becomes better and better with the number of attacker increases. This protocol only deals with out-sider attack and computation burden is high due to the use of public key cryptography.

4 IMPLEMENTATION

4.1 ALGORITHM

The algorithm for the Low Energy Adaptive Clustering Hierarchy (LEACH) implemented is :

Setup phase :

1. CN$\Longrightarrow$ r
2. If r < T(n) then, CH = CN else, goto step1
3. CH $\Longrightarrow$ G : id(CH) , join_adv
4. A(i) $\rightarrow$ CH(j) : id(A(i)) , id(CH(j)) , join_req
5. CH(j) $\rightarrow$ A(i) : id(CH(j)) , < t(i) , id(A(i)) >

Steady phase :

1. A(i) $\rightarrow$ CH(j) : id(A(i)) , id(CH(j)) , info
2. CH $\rightarrow$ BS : id(CH) , id(BS) , aggr_info

The various symbols used here are :

CN : candidate node to become the cluster head.

r : $randomvariable(0 < r < 1)$

T(n) : threshold value

CH : cluster head

G : all nodes in the network

id : identification number

join_adv : advertisement to join the cluster

A : normal node

join_adv : request to join the cluster

t : time–slot to send the sensed data

$\Longrightarrow$: broadcast

$\rightarrow$: unicast

4.2 NETWORK CONFIGURATION

[11] Here we have considered a heterogeneous network. A heterogeneous network is one in which all the nodes doesnt have equal energy. Let us assume that m fraction of the nodes have α times more energy than the other nodes and the total number of nodes be n. They are called as advanced nodes. Therefore,

Number of normal nodes = (1-m) × n

Energy per normal node = e_0

Number of advanced nodes = m × n

Energy per advanced node = e_0 × (1 + α)

Hence the total energy of the network is equal to ((1-m) × n) × e_0 + (m × n) × (e_0 × (1 + α)

The network configuration for the first simulation is as follows :

Field size = 100m * 100m

Number of nodes = 100

Energy per node = 1 joules

Election probability for a node to become the cluster-head = 0.15

Message size = 3000bits

5% of the nodes have double energy.

A few of the above parameters were changed for the required analysis.

The energy spend by any transmitter to send a L-bit message over a distance d is,

$$E_{Tx}(l,d) = \begin{cases} L \cdot E_{elec} + L \cdot \epsilon_{fs} \cdot d^2 & \text{if } d \leq d_0 \\ L \cdot E_{elec} + L \cdot \epsilon_{mp} \cdot d^4 & \text{if } d > d_0 \end{cases}$$

where E_{elec} is the amount of energy spent to run the circuit(of receiver or sender) for 1-bit data, ϵ_{fs} and ϵ_{mp} are the transmitter constants and depend upon the type of transmitter used and, $d_0 = \sqrt{\frac{\epsilon_{fs}}{\epsilon_{mp}}}$

The above network configuration, formulae and values of various parameters were referred from [11]

A few of the nodes in the network were compromised and selective forwarding was done. The cluster-heads were the nodes that were compromised. Now, the malicious

nodes would only forward only certain messages and dump the other. Hence the network throughput is expected to decrease and also abnormal characteristics of the network lifetime.

5 RESULTS

After a number of simulations, the following results were gathered. Based upon these results, a detailed analysis is presented.

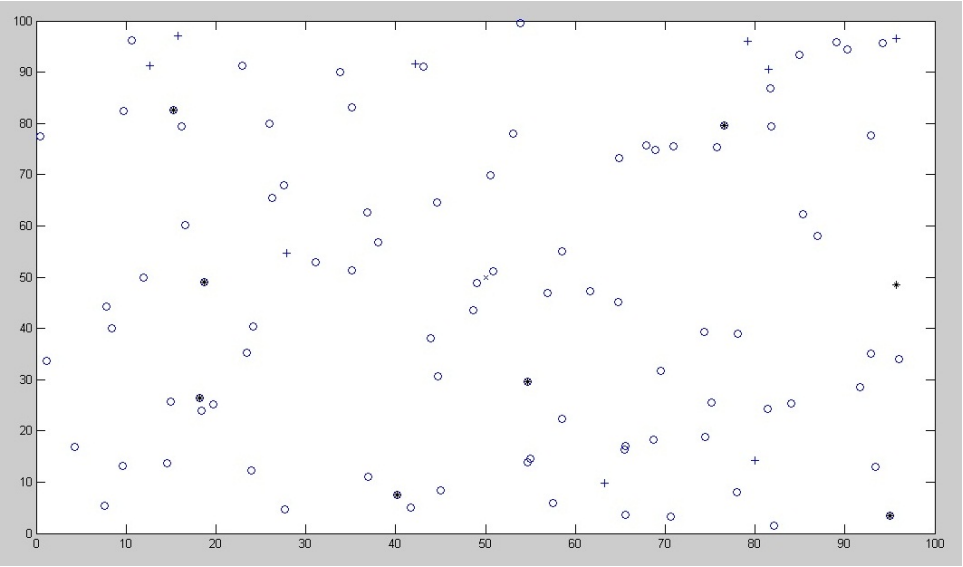


Figure 1: Field distribution-1

Figure-1 show the initial field distribution of the network, where LEACH protocol is implemented. A 100m*100m field is taken and nodes are randomly placed in it. The sink/base station, which is denoted by a $\times$, is placed at the center of the field (50, 50). Placing the base station at the center is convenient so that no node finds it out of its transmission range. Here, the advanced nodes are shown by a plus symbol (+) and the normal nodes by a circle ($\circ$) [11]. In Figure-1, all the nodes are alive in the network.

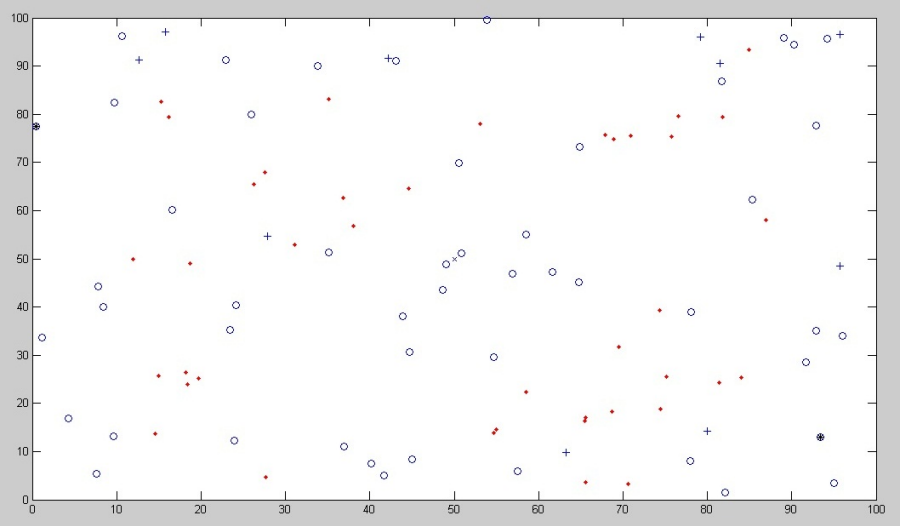


Figure 2: Field distribution-2

After a few rounds, a few of the nodes drains out all their energy. Such dead nodes are shown by the dot symbol (•) [11]. Such scenario is shown in Figure-2. The reason why some of the nodes drained out their energy before the others is because these nodes would have become the cluster-heads in the initial rounds of the data transmission. Since the cluster-heads have to aggregate the data and send it to the base station, which might be located far from the base-station, the cluster-heads use up their energy faster as compared to the non-cluster head nodes.

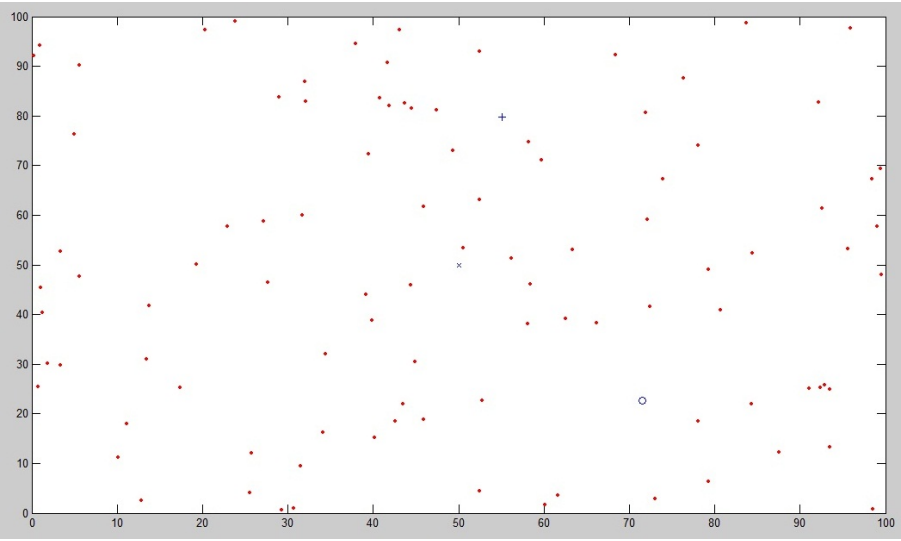
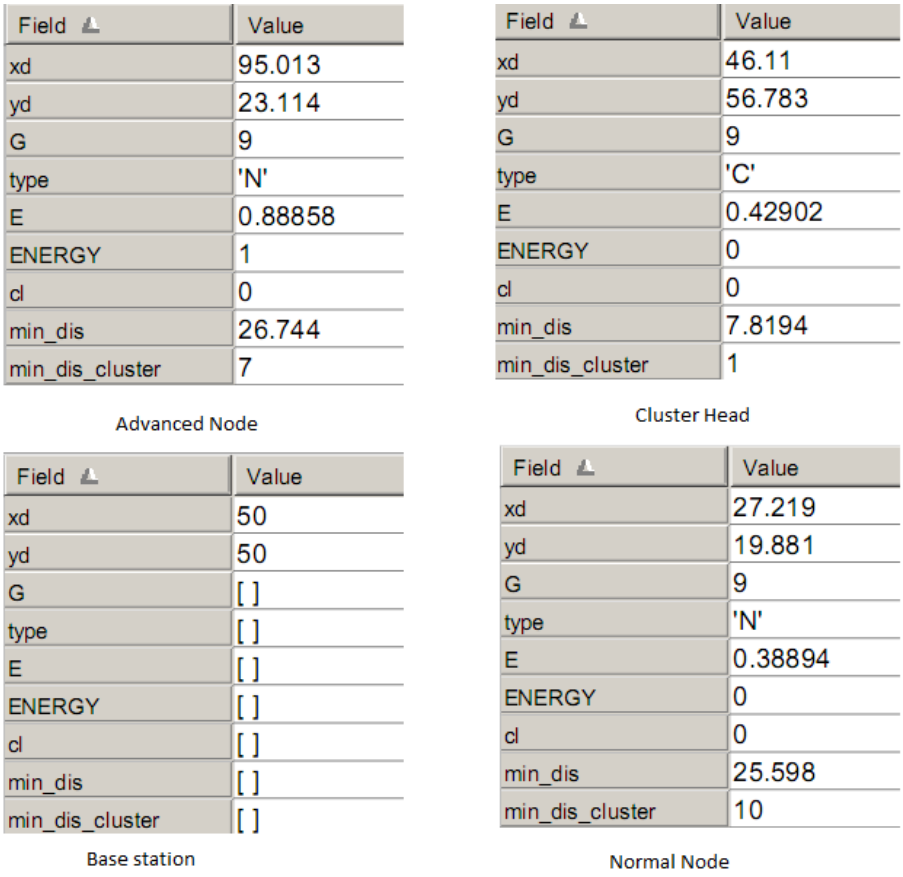


Figure 3: Field distribution-3

Figure-3 shows when all the nodes in the network die. The network ceases to work. No data is being transmitted or received either by the cluster-heads or the base-station.



Field	Value
xd	95.013
yd	23.114
G	9
type	'N'
E	0.88858
ENERGY	1
cl	0
min_dis	26.744
min_dis_cluster	7

Advanced Node

Field	Value
xd	46.11
yd	56.783
G	9
type	'C'
E	0.42902
ENERGY	0
cl	0
min_dis	7.8194
min_dis_cluster	1

Cluster Head

Field	Value
xd	50
yd	50
G	[ ]
type	[ ]
E	[ ]
ENERGY	[ ]
cl	[ ]
min_dis	[ ]
min_dis_cluster	[ ]

Base station

Field	Value
xd	27.219
yd	19.881
G	9
type	'N'
E	0.38894
ENERGY	0
cl	0
min_dis	25.598
min_dis_cluster	10

Normal Node

Figure 4: A snapshot of the node-values

A snapshot of different parameter values of the four types of nodes the normal node, the advanced node, the cluster-head and the base station, is shown in Figure-4. Meaning of different values is as follows:

xd : x-coordinate of the node.

yd : y-coordinate of the node.

G : chances of node becoming the cluster-head. If G¡=0, then only the node can be in the contention for becoming the cluster-head.

type : N denotes a non-cluster head node and C a cluster head.

ENERGY : if ENERGY=1, it means an advanced node and ENERGY=0 means a normal node [11].

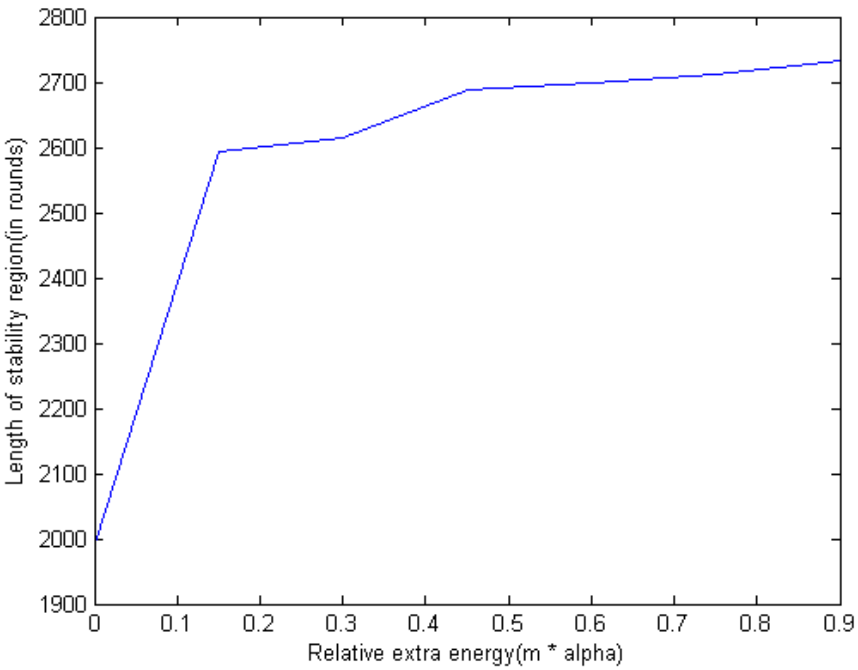


Figure 5: Stability

Stability region [11] is defined as the period in which all the nodes in the network alive. Its end is marked by the first dead node. The study of stability region is important because in LEACH protocol, the sender has faith on its corresponding destination i.e. the sender believes that the receiver will receive the message. Hence, the node doesnt know whether the other nodes in its neighbor are alive or not. This is not the case in location-based protocols where location information is exchanged between the two data exchanging nodes. Once the first node dies, cluster-head election and feedback remains unreliable for a long period of time. Figure-5 presents length of stability region, in rounds, for different degrees of heterogeneity or total relative extra energy i.e. m*α. It shows that heterogeneous networks are way more stable than homogeneous networks. For the current configuration, the length of the stability region is around 800 rounds for a homogeneous network. For a small degree of heterogeneity (m*α = 0.1), the stability regions length increases remarkably (to around 950 rounds). But increasing the total relative extra energy (m*α) doesnt keep increasing the stability regions length so drastically. The

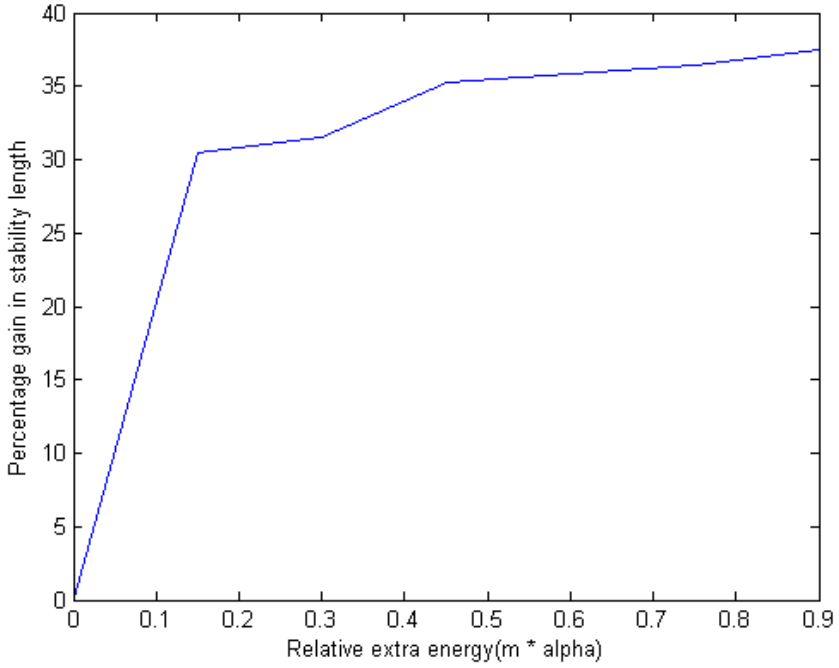


Figure 6: Percentage in stability gain

stability region can be extended up to around 35% extra by choosing an optimal value of m*α. This percentage increase in stability region is shown in Figure-6.

Figure-7 shows the lifetime for the 100m*100m sensor network with 100 nodes having 1.0 joule initial energy each and 5% of the nodes having double the energy i.e. 2.0 joule. The figure depicts the comparison between an uncompromised network and a network under selective forwarding attack. In the uncompromised network, all the nodes drain out their whole energy after 3000 rounds approximately. While in the compromised node, a few nodes are left with substantial energy, but with no use, as the malicious node wont be forwarding the nodes to the base-station. The network administrator will be in a state of confusion as it would appear that a few nodes have energy left but no information is received at the base-station. The adversary would intelligently forward information at timely intervals so as to avoid the risk of getting caught by the neighboring nodes.

Figure-8 shows the comparison between a homogeneous network and a heterogeneous network following LEACH as their routing protocol. In the homogeneous network, all the nodes have equal energy while in the heterogeneous network, 5% of the total nodes have

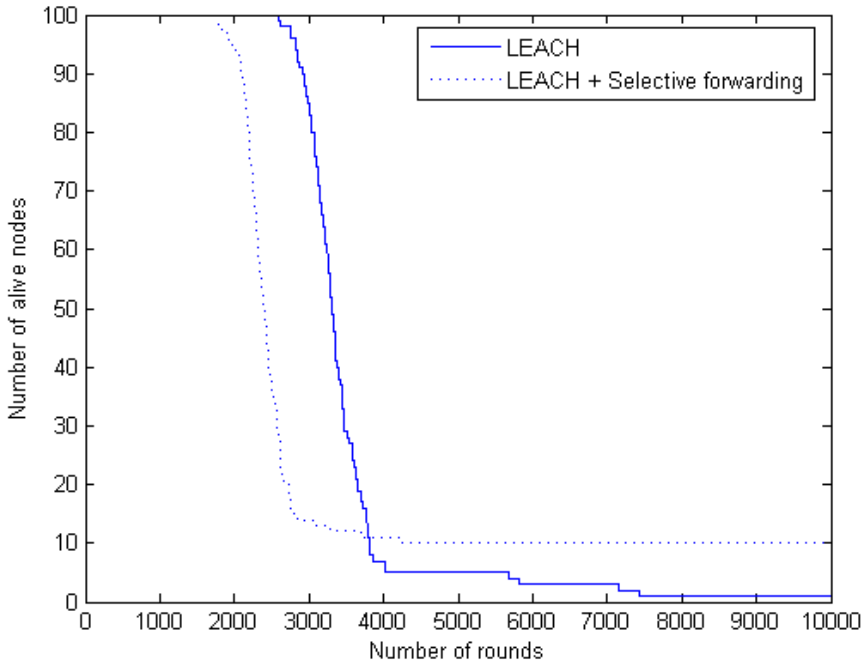


Figure 7: Network Lifetime

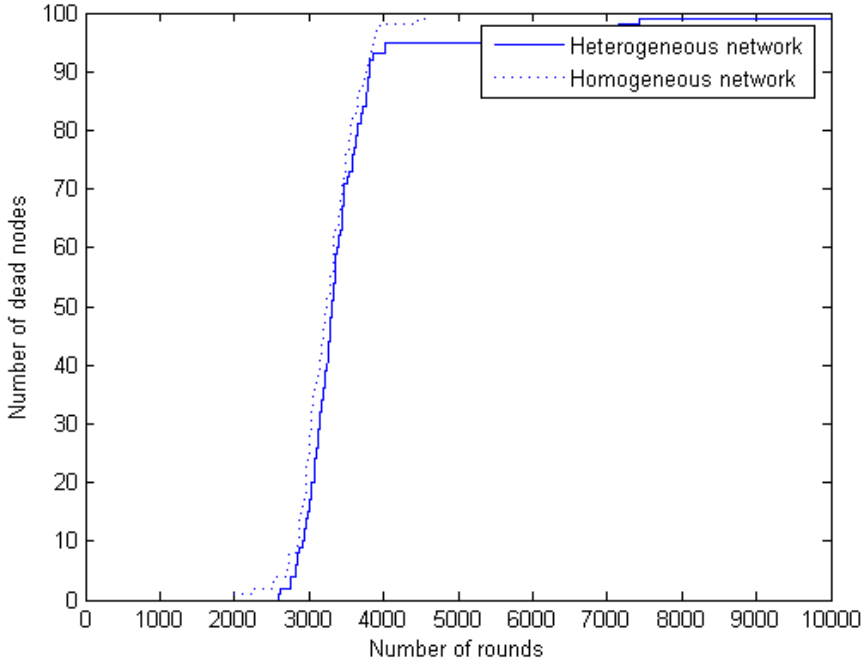


Figure 8: Comparison between hemogeneous network and heterogeneous network

double the energy than the other nodes. It was observed that the lifetime is increased in case of heterogeneous network. On increasing the heterogeneity i.e. m $\times$ α, the lifetime gets further increased.

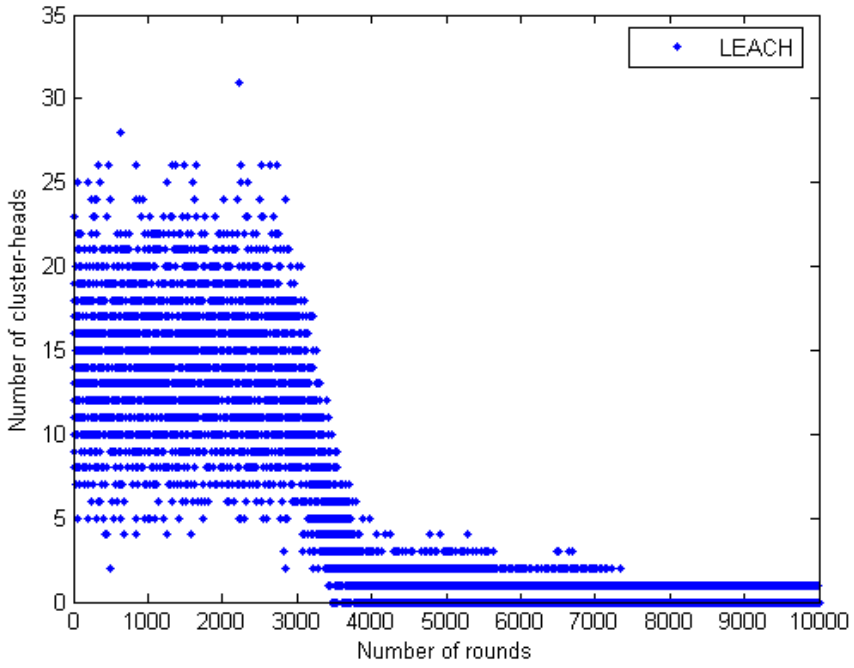


Figure 9: Number of cluster-heads per round in LEACH

Figure-9 and Figure-10 shows the number of cluster-heads per round for LEACH protocol and LEACH protocol compromised by selective forwarding attack respectively. Cluster heads in LEACH are selected by comparing the randomly generated number by the nodes in the contention for becoming the cluster-head, and, the threshold value. Hence, the LEACH protocol under the selective forwarding attack wont see much difference in this parameter. The number of cluster-heads slowly falls as nodes in the network starts getting dead and also the fact that energy required to perform the cluster-head tasks arent left with the nodes after certain iterations. A sudden dip is seen here because a number of nodes get dead in a quick interval. These are the nodes that became the cluster-heads in the initial rounds and hence, drained their energy very quickly.

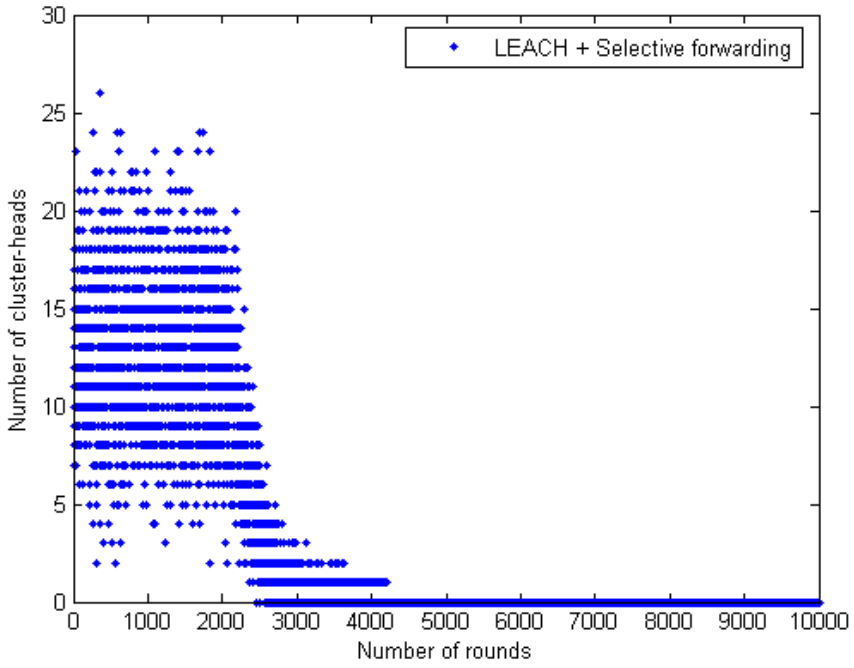


Figure 10: Number of cluster-heads per round in LEACH under Selective forwarding attack

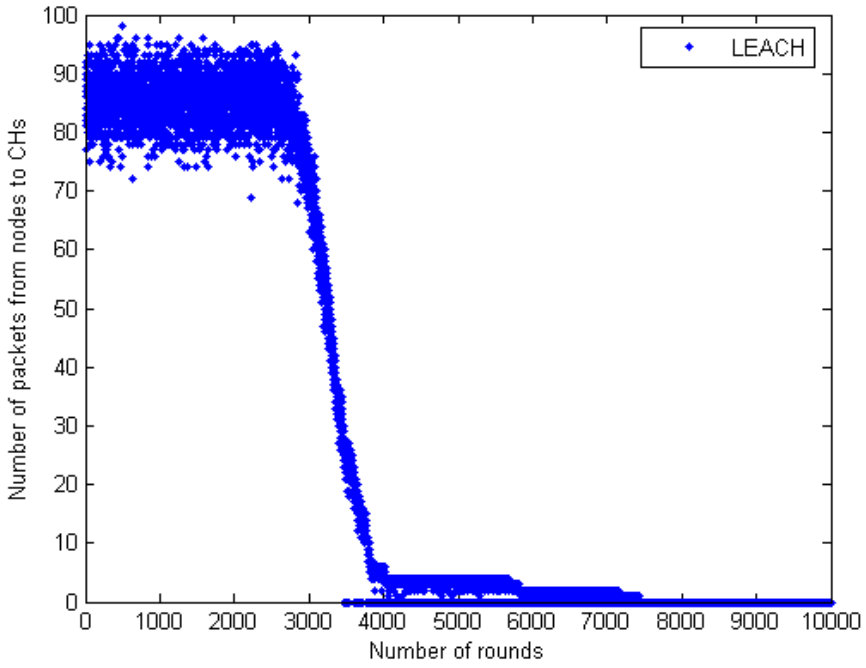


Figure 11: Throughput from nodes to CHs in LEACH

Throughput is the number of packets transferred per round. Figure-11, Figure-12 and Figure-13 shows the different throughputs of the network. Throughput is the parameter that is most affected by the selective forwarding attack. This can be seen by the difference in Figure-10 and Figure-11 i.e. number of packets transmitted from the sensor nodes to cluster-head gets decreased in case of networks compromised by selective forwarding attacker. As seen from the network lifetime graph (Figure-6), nodes are left with energy in the compromised network. But such network doesnt allow the forwarding of certain information to the other nodes. Hence decrease in throughput and less utilization of the energy.

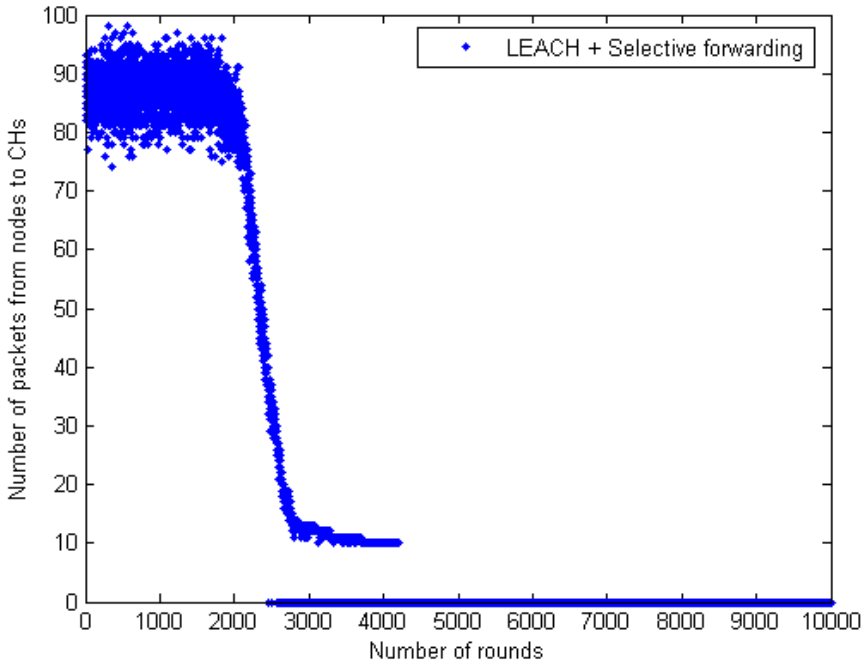


Figure 12: Throughput from nodes to CHs in LEACH under Selective forwarding attack

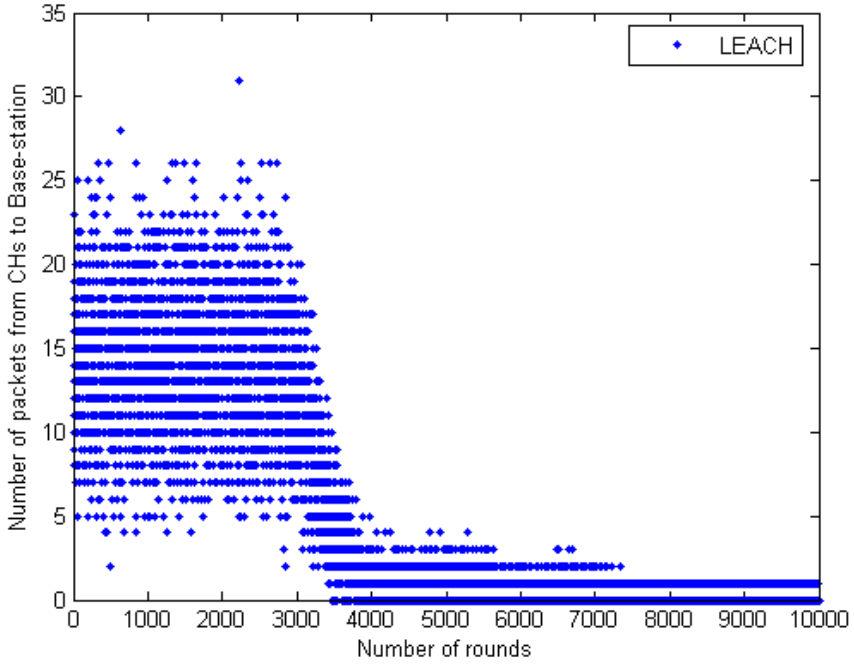


Figure 13: Throughput from CHs to BS in LEACH

6 CONCLUSION AND FUTURE WORK

In this thesis, we have discussed the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol and analyzed the protocol based on network lifetime, stability period and the network throughput. We have put light on the comparison of LEAH protocol with the effect of heterogeneity and selective forwarding attack.

In future, I would like to work towards overcoming the effects of selective forward attack by detecting it and providing essential countermeasures.

References

[1] L. B. Oliveira E. Habib H. C. Wong A. C. Ferreira, M. A. Vilaa and A. A. Loureiro. Security of cluster-based communication protocols for wireless sensor networks. In *4th IEEE International Conference on Networking (ICN05)*, volume Lecture Notes in Computer Science, pages 449–458, Washington, DC, USA, 2005.

[2] Jamal N. Al-karaki and Ahmed E. Kamal. Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications*, 11:6–28, 2004.

[3] Y. Geng C. Hong-bing and H. Su-jun. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. *China Universities of Posts and Telecommunications*, September 2008.

[4] G. Hu D. Wu and G. Ni. Research and improve on secure routing protocols in wireless sensor networks. In *4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008).*

[5] Wendi Rabiner Heinzelman, Anantha Ch, and Hari Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. pages 3005–3014, 2000.

[6] H. Zhang J. Chen and J. Hu. An eciency security model of routing protocol in wireless sensor networks. In *2008 Second Asia International Conference on Modeling and Simulation*, pages 59–64, Washington, DC, USA, 2008.

[7] C. Wang K. Zhang and C. Wang. A secure routing protocol for cluster-based wireless sensor networks using group key management. In *4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM08).*

[8] M. A. Vilaa H. C. Wong M. Bern R. Dahab L. B. Oliveira, A. Ferreira and A. A. F. Loureiro. Secleach-on the security of clustered sensor networks. (87(12)):2882–2895, December 2007.

[9] M. Bern R. Dahab L. B. Oliveira, H. C. Wong and A. A. F. Loureiro. Secleach - a random key distribution solution for securing clustered sensor networks. In *Fifth*

IEEE International Symposium on Network Computing and Applications, pages 145–154, Washington, DC, USA, 2006.

[10] A. V. Reddy R. Srinath and R. Srinivasan. Ac: Cluster based secure routing protocol for wsn. In *Third International Conference on Networking and Services*, page 45, Washington, DC, USA, 2007.

[11] Georgios Smaragdakis, Ibrahim Matta, and Azer Bestavrosl. Sep: A stable election protocol for clustered heterogeneous wireless sensor networks. *Proc. of the Intl Workshop on SANPA*, 2004.

[12] C. Karlof and D. Wagner. Secure routing in sensor networks:attacks and counter measures.*Ad Hoc Networks*, 1:293−315, May 2003.

[13] S.Zhu, S.Setia, S.Jajodia, LEAP:efcient security mechanisms for large scale distributed sensor networks,*10thACM Conference on Computer and Communication Security*, ACM Press, NewYork,2003,pp.6272