An Energy Efficient and Trust Aware Framework for Secure Routing in LEACH for Wireless Sensor Networks

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

Master of Engineering

in

Information Security

Submitted By

Arzoo Miglani

(801333003)

Under the supervision of:

Dr. Shivani Goel

Assistant Professor

Ms. Tarunpreet Bhatia

Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2015

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*An Energy Efficient and Trust Aware Framework for Secure Routing in LEACH for Wireless Sensor Networks*" in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Shivani Goel, Ms. Tarunpreet Bhatia* and refers other researcher's work which are duly listed in the reference section.

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

Signature:

(Arzoo Miglani)

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

(Dr. Shivani Goel)
Assistant Professor,
Computer Science and
Engineering Department

(Ms. Tarunpreet Bhatia)
Lecturer,
Computer Science and
Engineering Department

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. S. Bhatia)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my guide **Dr. Shivani Goel** and **Ms. Tarunpreet Bhatia,** Department of Computer Science and Engineering, Thapar University, Patiala, who has been concerned and has aided for all the materials essential for the preparation of this thesis report. She has helped to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research oriented venture.

I am also thankful to **Dr. Deepak Garg**, Head of Department, Computer Science Engineering Department, and **Ms. Jhilik Bhattacharya**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

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

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

Arzoo

Arzoo Miglani

ABSTRACT

Wireless Sensor Network (WSN) is an advanced technology and has been used widely in many applications such as health monitoring, environment monitoring, military purpose etc. Nature of this network is that they are often placed in an open environment and are susceptible to various attacks. Traditional cryptography methods are not supportable in WSNs as they have high energy and resource constraints. Trust management has been proved to be an effective measure to enhance security as well as to handle threats for WSNs. Trust can be defined as level of reliableness in a node. Low Energy Adaptive Clustering (LEACH) is a cluster based routing protocol for WSN which is superior to direct communication protocol and known for its minimum transmission energy. However, LEACH itself has some limitations related to security. In this thesis, an energy efficient and trust aware framework for secure routing in LEACH (EETA-LEACH), has been proposed that improves LEACH protocol by introducing trust to provide secure routing, while maintaining originality of LEACH protocol. This approach is a combination of trust-based routing module and trust management module that works together to select trusted Cluster Head (CH). The simulation results demonstrate that proposed scheme is better in terms of network lifetime and Packet Delivery Ratio (PDR). It is verified that malicious nodes will not be selected as CH and trust value of a malicious node decreases with time.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ADC	Analog to Digital converter
BS	Base Station
CH	Cluster Head
DoS	Denial of Service
EETA-LEACH	An Energy Efficient and Trust Aware Framework for Secure Routing in LEACH for WSNs
GEAR	Geographic and Energy-Aware Routing
HEED	Hybrid Energy Efficient Distributed Protocol
LEACH	Low Energy Adaptive Clustering
MANETs	Mobile Ad hoc Networks
PDR	Packet Delivery Ratio
PEGASIS	Power-Efficient Gathering in Sensor Information Systems
QoS	Quality of service
REQ	Request
SPIN	Sensor Protocols for Information via Negotiation
TEEN	Threshold sensitive Energy Efficient sensor Network protocol
WSNs	Wireless Sensor Networks

CHAPTER 1
INTRODUCTION

1.1 Introduction to WSNs

WSN is a network of large number of sensor nodes which are deployed over a region to monitor and to collect a certain amount of data, and when a large number of nodes work together they can measure a given physical environment and can be helpful in many ways. Each of sensor nodes are connected to one another. There may be a one to one relation or one to many. Sensor nodes can be deployed randomly or in a fixed or predefined way. In order to perform a collective measurement each of these nodes measure and collect the data and transfer to gateway (sink/BS) with the help of transmitting device. Data may be transmitted in a single hop (if node is directly connected to sink) or may be in multihop (if node and sink are not in direct contact). These nodes can be similar or heterogeneous; heterogeneous WSNs are that which consists of different type of nodes in a hierarchy. Architecture of WSNs is shown in figure 1.1.

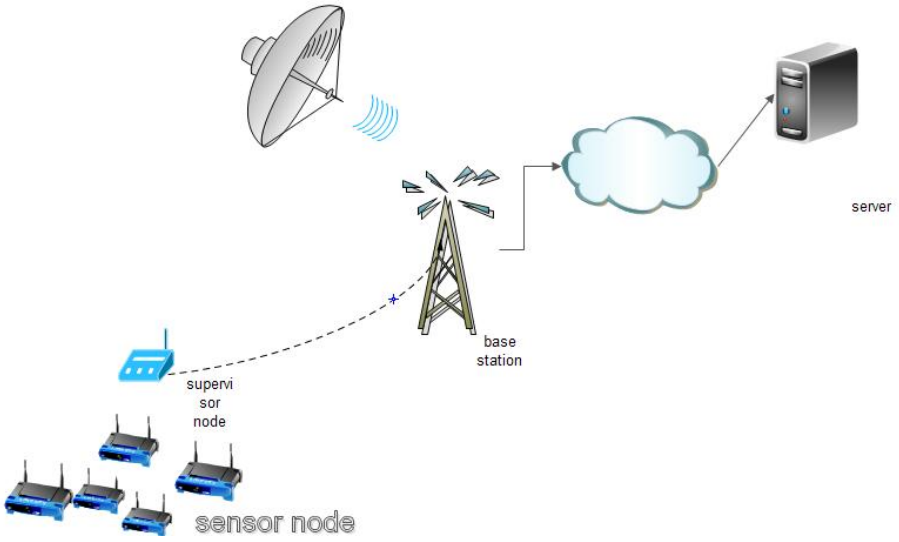

Figure 1.1: Sensor node architecture

It is a common misconception that WSNs are similar to ad-hoc networks though there is quite big difference between both of them.

- In sensor networks main issue is energy efficiency as there are more battery constrains but in ad-hoc networks there are not such tight constraints on battery.
- The number of sensor nodes used is much more than in an ad-hoc network.
- In ad-hoc networks, nodes show a high mobility but sensor nodes are less mobile.

- WSNs are application specific but ad-hoc networks are not.
- Sensor nodes are more exposed to failure.
- Sensor nodes mainly spread the message to all other nodes for communication as compared to ad-hoc networks that are based on one to one communications.
- Sensor node may not have a unique identification number because of huge number of sensor nodes as it is difficult to allocate a number to a large number of nodes.

1.1.1 Components of WSNs

A sensor node is made up of following components:

- A sensing unit
- A micro processing unit
- A power unit
- A transmitting unit or Transceiver unit

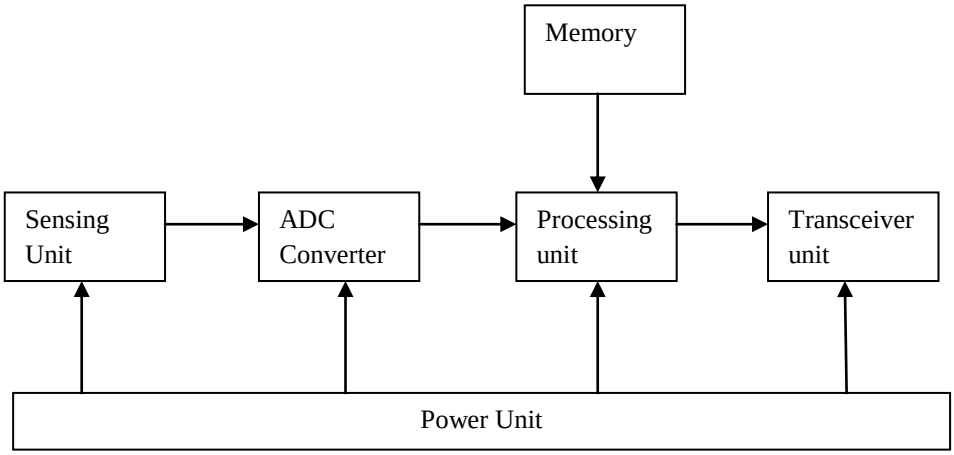

Figure 1.2: Components of sensor node

Sensing unit consists of a sensors which actually gather the sensory information and this sensing unit is further attached with ADC converter which convert analog signal to digital signal so that it can be fed to a microprocessor. **A sensor node** equipped with a transducer converts the physical motion into electrical energy and they are provided with a line of sight to communicate with other sensing node or gateway. **A processing unit** is used to make sensor nodes work with other nodes and they are provided with a storage device. **A power unit** is there to provide power to these sensors so that they could work and there are fewer sources to charge them. One of the available methods is to plant a solar cell as power source.

Also a much power is used by processing unit and transmitting unit, so energy efficiency is one of most critical issues of sensor network. **Transmitting unit** is used to transmit the signal to neighbouring nodes, sinks or internet. There will be a short range communication as there are energy constraints. It may be in transmit, receive, idle, sleep mode. It is advised to keep the nodes into sleep mode instead of active when it is not transmitting or receiving to save the energy. Handling of signal occurs in an easy way where comparison is carried, computed value is compared with a given threshold value and then that obtained value which is a analog value is first converted to binary form and send to gateway. Goal is to keep probability of computing false result low. The recognization of phenomenon of interest is done in a collaborative environment that is together with the sink .All other sensor nodes decide phenomenon of interest [1].

1.1.2 Types of WSNs

Based on deployment sensor nodes can be classified in two ways: structured WSNs and unstructured WSNs:

- **Structured WSNs**: In this network few sensor nodes are deployed at pre-planned locations. This type of networks is easy to manage as there is lower maintenance of network.
- **Unstructured WSNs**: These types of networks comprises of huge collection of sensor nodes deployed randomly in ad-hoc manner. It is difficult to maintain such a network, so these networks are left unattended to complete the tasks assigned to them. In addition it is quite difficult to identify faulty nodes with such networks [2].

1.1.3 Applications of sensor networks

Two main applications of sensor networks are monitoring and tracking. These two applications can be further expanded to following areas:

- **Environmental monitoring**: Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects, monitoring environmental conditions that affect crops, Forest fire detection, Flood detection etc.
- **Health applications:** Some of the health applications for sensor networks are setting sensors inside patient body so that doctors can monitor him even they are sometimes deployed to doctor’s body also so that their position can be located, diagnostics drug

administration in hospitals, monitoring the movements and internal processes of insects or other small animals.

- **Home applications:** Used to implement smart homes, As technology advances, smart sensor nodes and actuators can be buried in appliances, such as vacuum cleaners, micro-wave ovens, refrigerators, and VCRs to control them may be with respect to temperature or pressure.
- **Military**: For enemy tracing, for nuclear attack detection, battle damage assessment and for all these purpose we need to make these sensors fault tolerant and energy efficient.
- **Agriculture**: For finding the amount of pesticides best suited for crops, to analyze whether a crop is affected by insect etc.
- **Biomedical sensor applications**: Sensors are fitted in biometric device like finger scan, retina scan and they are very much helpful in identification.
- **Vehicular monitoring**: Sensor network can be located on roads or in vehicles in order to trace them and this will be beneficial in reducing accidents and maintain traffic.
- **Smart Kindergarten:** For teaching students at home a teaching environment is created where teachers can keep a eye on every student and also multiple activities are organised by student that help in overall development [3].
- **Pollution checking**: By installing a sensor device, pollution can be checked and this will make that city a smart city.

1.1.4 Challenges in WSNs:

- **Energy efficiency**: As sensor nodes are deployed in mass and generally deployed in areas where there are fewer sources for power such as forest, underwater, in sacks. This is one of the dominant key issues in WSNs. Most of the protocols, research have been proposed keeping this factor at the top. Multihop routing, keeping radio transceiver on idle mode are some of method to make the sensor nodes energy efficient.
- **Security**: As WSNs are deployed in open environment so they are prone to attacks like availability, spoofing, confidentiality, lack of integrity. In order to overcome this various algorithms have been proposed like trust management where a node accepts

data only from a trusted node, and problem of availability has been solved by making devices fault tolerant.

- **Routing**: Routing algorithms for wired network are not beneficial for WSNs as there are energy constrains and bandwidth constraints. Protocols like LEACH which works on concept of clustering where a CH is chosen and that CH will be responsible for delivering the data to sink node, SPIN works on concept that instead of broadcasting the message multicast the message only to those nodes which show their interest in the data and others like gossiping, flooding are also quite popular as they work keeping power constraints as a issue.
- **Fault tolerance**: Sometimes sensor nodes are meant to be placed in harsh environment. In that case nodes may get crashed because of environmental conditions, hardware failure, and software failure. Some nodes may be dead because of scarcity of battery. Because of those nodes sensor nodes whole network produced wrong result. So, we have to design such a network so that failures of those sensor nodes don't change functionality of whole network [4].
- **Localization**: Sensor nodes are deployed randomly in an infrastructure less manner that is without any predefined structure. After sensor nodes have been installed locating sensor nodes that are finding their actual location is very difficult. Determining the physical location of the sensors after they have been deployed is known as the problem of localization. A GPS device is being fitted to solve this problem. Localization methods should be able to discover errors or fault in nodes so that they can be corrected timely [5].
- **Data aggregation**: Sensor nodes work in collaborated manner. They collect data from their neighbouring nodes or other nodes and then deliver it to different nodes or sink node. So there are chances or data being duplicated which is an unwanted data that is just wastage of resources. Data aggregation algorithms are designed such that it aggregated data from various sensors and also removes extra data and data without duplicity that is only useful data is being hand over to sink node [6].
- **QoS**: As WSNs topology keeps on changing as compared to wired QoS services so those QoS methods are not supposed to be applied on WSNs and also not much of the work is being done in this area. So this can be a new research area. This area includes work on congestion, high throughput, low latency etc.

- **Synchronisation**: Time synchronisation is another important factor to adjust clock between nodes. In some applications like environment monitoring, vehicular monitoring, health monitoring it is important to keep the clocks synchronised, but while designing such software it is important to keep energy factor in mind, designed software or hardware should not rely on high use of power.
- **Hardware constraints**: A sensor node is made up of many components like processing unit, memory unit etc. These components should consume less energy, must be reliable and should occupy a less amount of space.

1.2 Routing Protocols in WSNs

Routing in WSNs is quite a difficult task because of several constrains associated with WSNs such as energy constraints, bandwidth constraints, memory constraints etc. Sensor network routing protocols are different from traditional routing as they are infrastructure less, uncertain and most importantly due to lack of energy resources protocols should be designed taking energy efficiency as a factor [7]. Some of commonly used routing protocols are being discussed below:

1.2.1 Data centric Routing Protocols

In address-centric routing protocols sensor nodes transfer data to sink without knowledge of other nodes i.e. there is no negotiation between nodes. Data-centric protocols is being different from conventional address-centric protocols as here after the nodes has send data to sink some midway nodes operate data aggregation on data which will help in removing data redundancy and also saves energy as there are reduced number of transmissions [8]. Some of data-centric protocols are: SPIN, ACQUIRE, Rumor Routing, COUGAR, Directed Diffusion, Information-Directed Routing, EAD etc. SPIN [9, 10] is the first data-centric routing protocol and is being discussed below:

Sensor Protocols for Information via Negotiation (SPIN):

Spin uses meta-data as a description for data which tells all information about data. Three types of messages are involved for communication with this protocol that is: advertisement (ADV), DATA and REQ. Whenever a sensor node has some data to route, first it will broadcast a ADV message to all its neighbour node by attaching meta-data of node. If neighbour node has interest with that data, it will unicast REQ message for that data. After

receiving a REQ message sender node will send DATA message that contains actual data to the neighbour node. Following the same procedure data could be routed to BS.

Advantages

- This protocol involves sending messages to its neighbouring nodes, hence classic flooding problem improved.
- As data is being carried out by intermediate nodes thus helps in reducing Data redundancy.

Disadvantages

- SPIN is not scalable
- Nodes which are deployed near to BS have to transfer maximum number of data packet. Therefore their energy level will get reduced [11].
- SPIN does not assure final delivery of data to BS, data may get lost somewhere in mid way if intermediate nodes are not interested in that data.

1.2.2 Hierarchical Routing Protocols

In the past few years, much of the research has been done in hierarchical routing area. In hierarchical routing protocol, nodes arrange themselves into a group of some nodes called cluster and there is one CH supervising every cluster. Nodes send their data to respective CHs which further route data to BS. Hence with these types of protocols, better energy efficiency could be attained. Some of popular Hierarchical routing protocols are: LEACH, TEEN, HEED, PEGASIS. LEACH and PEGASIS have been discussed below.

Low-energy adaptive clustering hierarchy (LEACH):

LEACH [12] is clustering based approach where nodes arrange themselves into local area called clusters. Each cluster is supervised by a CH; nodes send data to CH and CH after aggregation further route data to BS. LEACH has several rounds for executing routing, after every round a new CH is selected to balance energy load. Every new round starts with Set-up phase proceeded by Steady-state phase. In Set-up phase clusters are formed based on some threshold value and next sensor nodes will decide which CH to choose based on signal strength. Threshold value is given by equation:

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

Based on signal strength nodes decide which CH to choose. In next step, after clusters have been formed based on strength of sensor in a cluster, CH will form a TDMA schedule and

each node is supposed to transmit data to CH in their respective slot only. Figure 1.3 shows cluster formation in LEACH.

Advantages:

- LEACH is energy efficient protocol
- LEACH increases lifetime of the network

Disadvantages:

- CH energy consumption is high
- After a time period, it is likely that a node with low energy may get selected as CH [14].

Power-Efficient Gathering in Sensor Information Systems (PEGASIS):

PEGASIS [13] protocol is an improvement of LEACH. Unlike LEACH which is clustering based, PEGASIS is chain-based protocol. Greedy technique is used for formation of chains. In this protocol, instead of cluster formation chain is formed so that each node communicated with its neighbour for transmitting and receiving packets instead of sending data directly to CH. Data moves in a chain from one sensor node to other in linear fashion. After every round a sensor node is randomly selected to aggregate and transfer non-redundant data to CH.

Advantages:

- PEGASIS has reduced overhead of formation of dynamic CH.
- Total number of transmissions has been decreased, hence increasing network lifetime.

Disadvantages:

- Overhead in calculating remaining energy of every neighbour.
- For a distant node there could be delay in routing data.

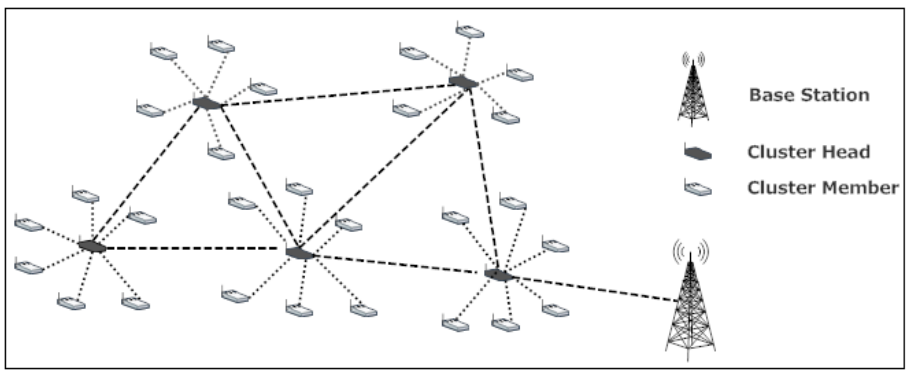

Figure 1.3: Cluster Formation

1.2.3 Location-based Routing Protocols

In this protocol sensor nodes are identified by means of their location or area. Node that is placed within a given area will be welcomed as receiving node. The main advantage of location-based routing is, it consider mobility of sensor nodes. In addition these networks works best when density of sensor nodes is increased. Nodes need to calculate location information of other nodes in order to estimate the distance between sensor nodes so that energy consumption can be balanced. Some of location-based protocols are: TBF, MECN, BVGF, Span, SMECN, GAF, GEAR. One of popular routing protocol names GEAR is being examined below:

Geographic and Energy-Aware Routing (GEAR):

Every node runs with a hardware equipment to calculate current positions of nodes. In addition nodes also keep track of their own residual energy as well as residual energy of their neighbours. The actual cost of route is packet is judged by aggregation of residual energy plus distance between source and destination. There are two stages in this protocol: First is routing packets approaching to the target area, then to send the packet within the area.

Advantages:

- GEAR is energy efficient.
- GEAR performs better in case of PDR.

Disadvantage:

- Overhead in calculating distances and residual energies of other nodes.

1.3 Attacks in WSNs

Attacks in WSNs can be classified as active and passive attack [15]. In passive attack adversary may perform operations like traffic analysis also known as sniffing. Passive attacks are less destructive than active attacks and it will only lead to discovery of important information without permission from anyone. In active attacks, attacker will perform actions that will lead to malfunctioning of WSNs like DoS attack, forgery. Various attacks in WSNs are:

- **Sinkhole attack**: In Sinkhole attack, an adversary node may pretend itself as a legitimate sink node and tries to attract almost all traffic passing from a particular region, which could result in false routing. As shown in figure 1.4 malicious node is attracting traffic from all nodes.

- **Blackhole attack**: In this attack, malicious node will drop all packets routed to it that it should forward to receiver. Refer figure 1.5, malicious node is discarding all packets that it is supposed to forward.
- **Greyhole/Selective forwarding attack:** It is similar to Blackhole attack only difference is instead of discarding all packets compromised node would discard only specific selective packets (like routing packets). Refer figure 1.6.
- **Wormhole attack:** A pair of adversaries will form a tunnel between them and collect packets from one part in network and it will replay those packets somewhere in another part of network. Refer figure 1.7, attacker 1 and attacker 2 are forming a tunnel between them to disrupt normal functioning of WSNs.
- **Sybil attack:** In this attack, malicious node will create fake IDs of other nodes and then impersonate as real nodes of network. As shown in figure 1.8, adversary node is advertising itself as A or B or C.
- **DoS attack:** Here attacker will flood the node with tons of useless REQ message so that node gets busy in replying those REQ messages, forgetting its other important tasks intended for WSNs. Refer figure 1.9.

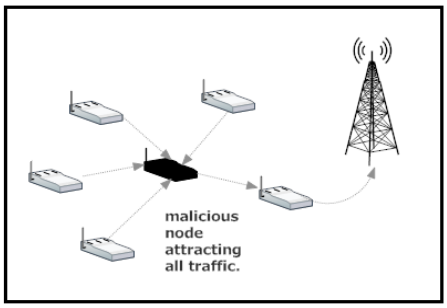

Figure 1.4: Sinkhole Attack

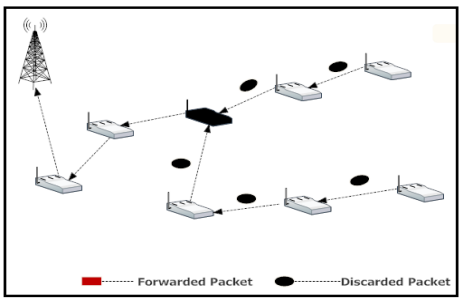

Figure 1.5: Blackhole attack

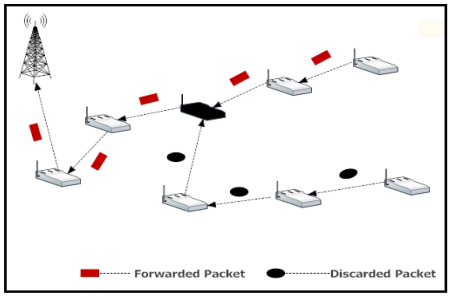

Figure 1.6: Greyhole Attack

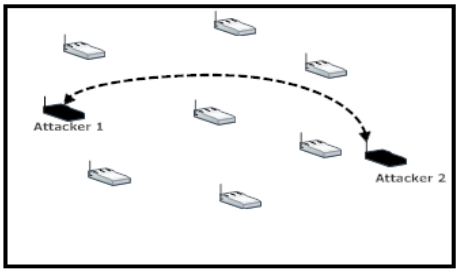

Figure 1.7: Wormhole Attack

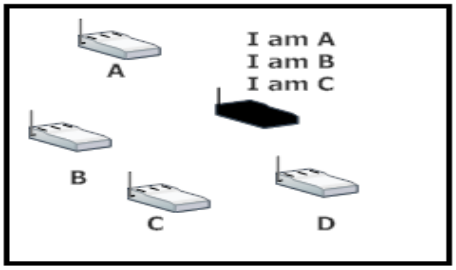

Figure 1.8: Sybil Attack

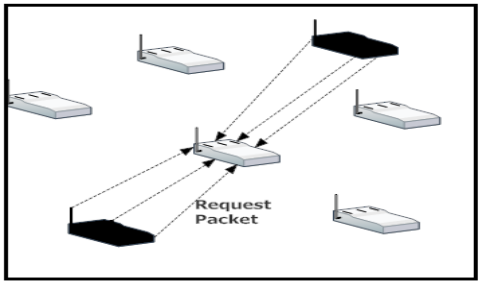

Figure 1.9: DoS Attack

1.4 Importance of Security in WSNs

WSNs are deployed in an open environment and hence are susceptible to various attacks. A node may get compromised and disrupt normal functioning of sensor network. In specific applications of WSNs like health monitoring, military, vehicular monitoring in which life is a critical issue, compromised network is not tolerable. Consider a scenario where doctor examines a person remotely, in this case compromised sensor nodes will not be acceptable. In addition, WSNs support multihop path routing and being in an unsecure environment there are chances of packet drop, wrong path selection which would adversely affect performance of WSN. The attacks discussed above could lead to abnormal functioning of sensor networks. So it is necessary to prevent sensor networks from adversary attacks to perform normal functioning. In order to save WSNs against various attacks cryptographic techniques, trust management schemes and intrusion detection system has been proposed. Each of these proposed solutions have their own advantages and disadvantages.

1.5 Motivation of Thesis

With the evolution of third wave in computing called ubiquitous computing, the demand of assuring security solutions are getting more attention than ever before. Ubiquitous computing is a concept of software engineering, where people can interact with computers anywhere, anytime whenever they need [16]. WSNs are one of example of ubiquitous computing.

Researchers are focusing on finding security solution for WSNs. A cryptographic solution requires high computational capacity, power and resource. As sensor networks are open and dynamic in nature. So it is easy for an adversary to compromise network and steal keys, thus making network an unsecure network. Hence, Traditional methods of cryptography such as TinySec [17] can be used in prevention of external attacks but they cannot block internal attacks. So, trust management could be a solution to security problems. The main motivation

in studying trust management is to establish a secure communication so that WSNs can be used safely without interruption of any adversary. Most of the trust based security solutions in WSNs consumes a lot of energy. In this thesis an energy efficient solution is provided to calculate trust. LEACH which is itself an energy efficient protocol is used for routing with some changes in it which makes it more secure and more energy efficient.

1.6 Thesis outline

The rest of the thesis is organised as follows: Chapter 2 describes introduction and taxonomy of trust management. Also it describes about the most relevant existing work in flat and clustered trust management schemes. Chapter 3 describes about problem statement. Chapter 4 explains about simulator used for results. Chapter 5 explains proposed work. Chapter 6 presents simulation results and discussion. Chapter 7 concludes the proposed work and discusses future work.

CHAPTER 2
BACKGROUND AND RELATED WORK

2.1 Introduction to Trust Management

Trust can be explained as a belief in reliableness of other node i.e. how much a node has confidence in establishing a secure communication with other node. Calculated value of trust can be further used by higher layer to take decision such as CH election [18, 19], reliable routing [20, 21], and data aggregation [22]. By implementing a trust based mechanism several problem like forgery, authentication, sniffing, unauthorized access can be solved and a secure routing could be implemented. Some of trust characteristics are given below:

- Subjective: Trust is being calculated based upon observations and recommendation concluded from past actions.
- Asymmetric: If one node X has trust on other node Y, it does not imply that Y should also trust X. Trust calculated between X and Y are independent.
- Dynamic: Trust may change after some time depending on nodes behaviour. In addition trust may also change in case if node is mobile.
- Reflexive: A node should trust itself
- Incomplete Transitivity: If X trust Y and Y trust Z, it may be possible that X distrust Z depending on behaviour of Z.

2.2 Taxonomy of Trust Management in WSNs

In this section, some common terms used in WSNs have been discussed in the form of classification based on nature of different parameters. Figure 2.1 illustrates parameters considered.

2.2.1 Based on Technique used for rust calculation:

Here, various canonical methodologies have been discussed that are used for computing trust.

- **Bayesian Probabilistic based trust model:** It can be distributed in two views: objective and subjective view. In objective view, probability is calculated purely

based on data analyzed [23] and in subjective view probability expresses a personal belief [24]. By using a Bayesian theory, uncertain trust values can be assigned rather than assigning 0 or 1. Trust values are dependent on past action and on other nodes behaviour, thus producing uncertain data. So, Bayesian probability is best suited for calculating trust in WSNs.

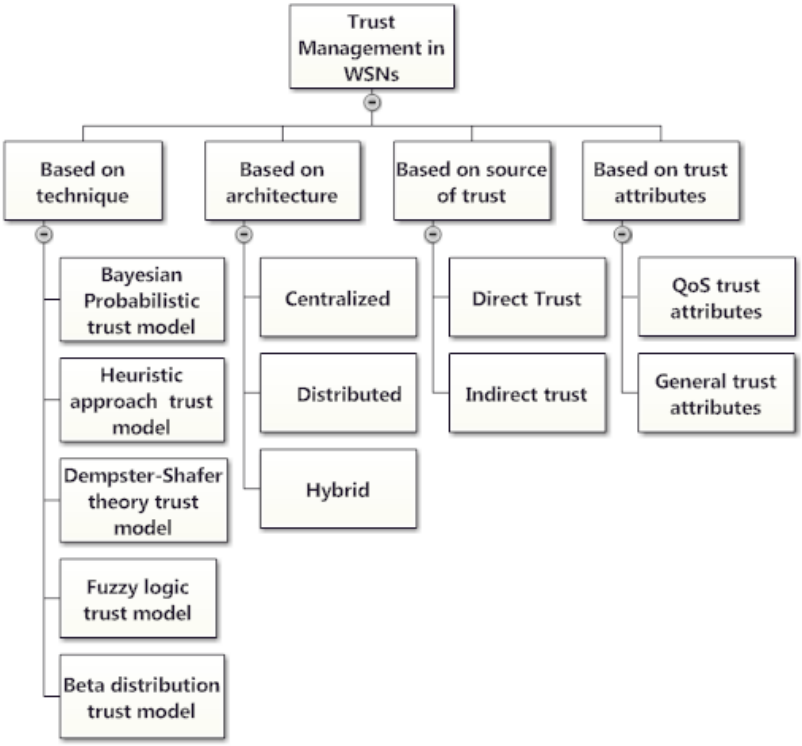

Figure 2.1: Taxonomy of trust management in WSNs

- **Heuristic approach based trust model:** By using a heuristic approach, optimal solution may not be obtained but definitely a solution with less computational overhead and in less time will be obtained. The most common example by which heuristic can be explained is hit and trial or rule of thumb. Trust may be calculated by implementing a series of if-else statements to find a solution (HATWA model by Dhulipala et al. [25]).
- **Dempster-Shafer theory based trust model:** Dempster-Shafer theory of evidence is an abstraction of Bayesian probability theory. It is based on belief functions and plausible reasoning, which aggregates information from different sources to calculate probability and thus satisfying requirement of trust management [26]. In addition, it is based on the fact of getting mass or degrees of belief for one argument from subjective probabilities for an associated argument.

- **Fuzzy logic based trust model:** As mentioned earlier, nature of trust values is uncertain so they cannot be simply assigned with true or false value. However, fuzzy logic is a type of multi-valued logic to deal with reasoning, that gives an imprecise solution rather than exact. There are some rule in trust algorithm compromising of if statements and based on those statements decisions on trustworthiness of nodes are taken.
- **Beta distribution based trust model:** It deals with uncertainty related to probability of success. It can be treated as a mechanism to calculate and update trust values obtained directly or indirectly. The benefit of the beta distribution trust model is flexibility that works on the statistical approach. Trust computation validity is determined by mapping the beta distribution to an opinion that will help in deciding beliefs in success of that event or statement [27, 28]. The probability density function (PDF) is used to compute trust values and it can be defined by following equation:

$$f(x|\alpha,\beta) = \frac{1}{B(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1}, \qquad 0 < x < 1, \alpha > 0, \beta > 0$$

Where,

$$B(\alpha,\beta) = \int_1^0 x^{\alpha-1}\,(1-x)^{\beta-1} dx,$$

$$0 < x < 1, \alpha > 0, \beta > 0$$

And the probability expectation value of beta can be expressed as:

$E(x) = \frac{\alpha}{\alpha+\beta}$, where α, β are number of positive and negative results.

2.2.2 Based on Architecture

Here framework for calculating trust is discussed:

- **Centralized:** In this architecture trust is calculated by a central node (it may be a BS). The advantage of using centralized model is this it doesn't require consumption of high energy but on a negative side there is dependency on a single node and if that intermediary or central node gets compromised or collapsed then there is no use of a trust model. Storage computation on central node would also be high with this architecture.
- **Distributed:** Unlike centralized framework, there is no dependency on a single node, here sensor nodes compute trust by themselves. But this model may lead to high energy consumption which itself is a dominant key issue in WSNs.

- **Hybrid:** Taking best of above described models, some approaches used hybrid model where within a group or a cluster distributed approach is used and evaluated result from each sensor node is sent to head of group to calculate the final trust.

2.2.3 Based on Source of rust

Various methods of trust aggregation have been discussed here:

- Direct trust: If two nodes are neighbour or they are in communication range of each other, they can calculate trust directly via eavesdropping, overhearing or snooping. Direct trust computed by node itself is always reliable, thus fake recommendations are not possible in this case.
- Indirect trust: It is not possible for every node to calculate trust of every other node, sensor nodes may use trust evaluation result of other node in order to save energy and communication overhead. However, before considering recommendations from other nodes, it should be checked that whether node providing recommendation is itself trustworthy or not.

2.2.4 Based on trust attributes considered for trust composition

Here, trust attributes that are used by various authors to compute trust are discussed.

- **QoS trust attributes:** This include those attributes that affect quality of network. Attributes like network loop discovery, security of network, delivery ratio, reliability of network, co-operation between nodes, task execution, efficient routing, energy level etc. are all included in this category. Schemes introducing these attributes will compute trust based upon quality of network. More the node is perfect in performing these QoS affecting tasks more trustworthy it is.
- **General trust attributes:** Most of the trust schemes are based upon QoS trust attributes. But some schemes also considered general trust. In other terms it can be called as friendly trust or social trust [29, 30]. This includes attributes like goodness, faithfulness, associativity, privacy, number of interactions etc. Though less work have been proposed in this field, in future work could be extended considering these attributes.

2.3 Attack specific to Trust Management Systems

- **Bad mouthing attack:** While accepting recommendation from a node it may so happen that some nodes may regard a good node as a bad node that has described them as bad node earlier. Refer figure 2.2.
- **On-off attack:** In this attack, a sensor node strategically can behave well alternatively although it is a bad node. This is possible if trust is calculated using old trust values where bad node can balance its activities with good activities. In order to overcome on-off attack, previous calculations should not carry higher weights than that of used in present calculation or not to use any previous calculation [31]**.** Refer figure 2.3.
- **Conflicting behaviour attack:** A node may pretend good to some nodes while behaving badly towards other nodes which may mislead average recommendation. This attack often occurs in a trust management model.

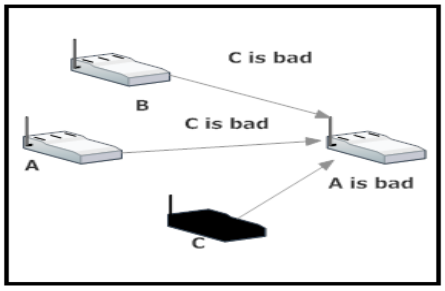

Figure 2.2 Bad mouthing attack

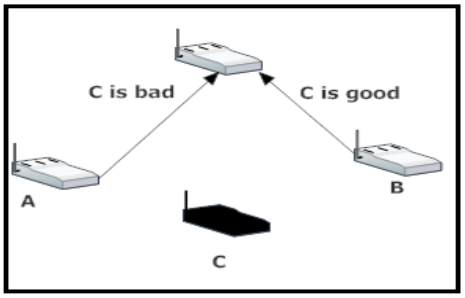

Figure 2.3 On-off Attack

2.4 Literature survey

This topic introduces about the most relevant existing work in flat and clustered trust management schemes literature which are described as:

2.4.1 Cluster-based WSNs trust models

While talking about cluster based approach in WSNs, LEACH is the first protocol that strikes in mind. Fei Song et al. proposed a Trust-based LEACH protocol [32] which is an extension of existing protocol LEACH [33], a trust factor is added to LEACH for secure routing. This proposal consists of two main modules: trust management module for examining neighbour's action and trust based routing module which enables safe routing by using results from trust management module. Monitoring module monitors behaviour according to nature of situational operation (sensing, routing, data aggregation etc.) and in trust evaluation module,

based on report from monitoring module direct and indirect trust will be calculated by following equations respectively:

$$DT(i,j,O_A) = \frac{N_o + 1}{N_o + N_m + 2},$$

$$IDT(i,j,O_A) = TS(i,k,O_A) \times ST(k,j,O_A) + \left(1 - TS(i,k,O_A)\right) \times TS(i,j,O_A)$$

Where, O_A is situational operation; N_o, N_m are number of good and bad behaviours respectively; ST is second hand trust value and *TS*(*i*, *k*, *OA*) and *TS*(*i*, *j*, *OA*) are the situational Trust of node *i* on node *k* and node *j* respectively. Once direct and indirect trust are calculated, new trust is updated and different weights are assigned to new trust and old trust to resist on-off attack. However, for routing purpose, important characteristics of original LEACH protocol are maintained as it is with minor changes by adding trust functionality. In actual protocol nodes decide which CH to choose based upon signal strength but in TLEACH CH with maximum trust value are chosen. Future research can be done with this topic by further reducing overhead.

Another model with same motive of improvement in LEACH is proposed in [34] by Fei et al. In Improvement of LEACH Routing Protocol Based on Trust for WSNs (LEACH-TM) node with energy higher than threshold will only be eligible for selection of CH and its equation is given by:

$$E_{th} = E_o * \left[1 - \theta^{(n-r)}\right]$$

where, E_{th} is threshold energy for round r, E_o is initial energy of node, r is the current round; n is expected total number of rounds and θ is energy attenuation factor. If we use this method for CH selection, nodes with less energy will not get selected as CH. Once a node has decided itself to be a CH, it will start finding its close CH neighbour by equation:

$$\mathrm{L} = \emptyset \times \sqrt{\frac{1}{\pi K}} \times M$$

where $\emptyset$ is an adjusting factor, K is total number of CHs and M is detected side length of square area. If distance of node to neighbour CH is less than L then this neighbour node is selected as close CH. In next step CH will calculate weight of each close neighbour CH by:

$$W_{ch} = \alpha \times \frac{E_{Rem}}{E_{Int}} + \beta \times \frac{T_{node}}{\sum T_{node}} + \gamma \times clusters$$

E_{Rem} is remaining energy of node , E_{Int} is initial energy of node, T_{node} is trust value of node, $\sum T_{node}$ is sum of trust of all close neighbour and α, β, γ are weight factors and clusters is number of time node is selected as CH. Then node with heaviest weight will be chosen. After this step all CH will be designated. Now node will decide which trusted CH to chose and it would be given by:

$$\widetilde{W}_{ch} = = \ x \ \times \frac{E_{Rem}}{E_{Int}} \ + \ y \ \times \frac{T_{node}}{\sum T_{node}} + \ z \times \frac{d(node, CH)}{D_{n-CH}}$$

Where $d(node, CH)$ is distance between node and CH and D_{n-CH} is maximum permitted distance between node and its CH and its value is a constant and x, y, z are weight factors where x+y+z=1. Based upon these trust values trusted path will be selected for multipath routing.

Bao et al. proposed a hierarchical trust management scheme [30]. In this model three main factors of trust management are trust composition (i.e., what trust attributes are to be considered), trust aggregation (i.e., how to calculate trust from trust attributes) and trust formation (i.e., how trust is generated from each trust attribute). Advantage of this approach is this it has considered social trust along with QoS trust factors. Social trust attributes include intimacy for computing amount of past interaction between two nodes, honesty for analysing suspicious activity and energy and cooperativeness are being considered for computing QoS trust. Trust will be calculated based on following equation:

$$T_{ij}^{X}(t) = \begin{cases} (1-\alpha)T_{ij}^{X}\ (t-\Delta t) + \ \alpha T_{ij}^{X,direct}(t) \\ if\ i\ \ and\ j\ are\ 1-hop\ neighbors; \\ avg_{k \epsilon N_i}\{(1-\gamma)T_{ij}^{X}(t-\Delta t) + \ \gamma T_{kj}^{X}(t)\}, \\ otherwise. \end{cases}$$

Where $T_{ij}^{X}(t)$ is the trust value updated by node *i* for node *j* and α is used to set whether old values or new trust values will be given preference (a larger α means present trust will be given high weightage), X represent trust attribute. Total trust will be calculated by aggregating trust values from all trust attributes. This scheme has also proposed trust based IDS as well as trust based geographical routing and both of the applications outperform traditional methods.

Rather than relying on optimal solutions Dhulipala et al. proposed A Heuristic Approach Based Trust Worthy Architecture [25]. This model has taken mobility of nodes into account for better trust aggregation. Moreover, this approach has made a comparison with Group-based trust management scheme (GTMS) [35] which is also a hybrid trust architecture model. Distributed trust is calculated within a cluster where every node calculates trust of every other node and centralized trust is calculated based on overall cluster performance. If more than 80% of nodes are trusted then cluster will be declared as a secure for communication. For evaluating trust a network monitoring node is placed outside every cluster which calculates trust based on past interaction. Network monitoring module first applies security model that will decide trust value based on authentication and encryption process , then it applies

mobility model where energy consumption during mobility of node is taken into account and finally it applies reliability model, where data fusion, negligible packet loss, less delay and energy cost during transmission and receiving of packets are key parameters. At node level, trust will be calculated by applying specified algorithm which first checks trust by successful and unsuccessful interactions and if it is not adequate then calculate trust for security model and even if it is not adequate then calculate trust in mobility model if node is not static followed by reliability model, then if mobility trust is not enough for communication and at last calculate overall trust even if reliability trust is not ample. But there is no method described for case where network monitoring node gets compromised. It is assumed that network monitoring node will never get compromised.

Compared to HATWA model where a network monitoring node is required, A Light Weighted Data Trust Model is proposed by Na Wang et al. [36]. In this model data values of neighbouring nodes are compared and those nodes whose sensed data values are not consistent with other nodes are declared to be faulty node. Similarity between nodes is calculated by relation $s_{i,j} = \frac{X_i X_j}{X_i^2 + X_j^2 - X_i X_j}$, X_i, X_j are sensed value of i and j respectively and all these recording are stored in CH. For calculating direct trust successful interactions will be checked within a specified period and in case it had interactions, number of similar data comparison are compared with 5, if they are less than 5 then it is considered as invalid. Remaining energy is checked after this and if it is greater than 10% indirect trust model is applied. For computing direct trust and indirect trust, CH feedback which is stored in a matrix is used and given by relation respectively.

$$IT_{x,y} = \frac{I_{x,y} * S_{x,y}}{10} \, , DT_{ch,y} = 10 * \frac{s_{x,y} + 1}{s_{x,y} + d_{x,y} + 2}$$

Another fuzzy based model is presented in [37] for secure routing. Initially CH will be selected based upon remaining highest energy. A trust monitor and energy watcher is supported by every CH. After selecting a CH, every node share a master key which is used when there is broadcast by BS and a cluster key is shared by every cluster member. Based upon broadcast from BS and loop discovery, trust monitor will calculate trust values of cluster member and energy watcher will calculate cost in delivering packet from that node to BS. However by applying fuzzy rules trusted path will be selected by CH to forward packet.

Sakthidevi et al. [38] proposed a Fuzzy Based Trust-Aware Routing Framework for dynamic WSNs. The main motive of this proposed scheme is to reduce energy consumption as well as to solve data aggregation problem. On every node three parameters are analyzed i.e. energy

consumption by energy watcher, trust level by trust manager, distance of node to CH by distance estimator. After analyzing the above mentioned factors series of fuzzy it-then rules are then applied on the values observed. Final results are calculated based upon output of aggregation of equivalent members of fuzzy of considered parameters. Simulation results proved that with this scheme PDR, throughput and energy efficiency is improved.

J. Manickam et al. [39] proposed another fuzzy based solution. This scheme has less overhead with respect to energy and memory consumption. Trust is calculated at both intra-cluster and inter-cluster level. Inside a cluster to reduce communication overhead only direct trust is calculated. At inter-cluster level both of direct as well as indirect trust is calculated. Direct trust is calculated using a sliding time window scheme. For calculating indirect trust recommendation are considered, for requesting a recommendation a trust request (TREQ) message is broadcasted to all neighbours whosoever comes in transmission range. For deciding final trust fuzzy if and then rules are applied to three parameters that are: direct trust, recommendation inconsistency and number of fluctuations.

2.4.2 Flat WSNs trust models

A trust model using fuzzy logic is being proposed by Tae Kyung Kim and Hee Suk Seo [40] which is a centralized scheme. A BS is used to calculate reputation value of other community member node. In order toreduce uncertainty, aggregation of fuzzy output data is considered to choose most trusted path for routing but in this case there are chances of loosing data. However, on flip side there is a bottleneck on centralized node and also an issue with storage i.e. where to store past reputation values of nodes.

Zhan et al. proposed a popular model TARF [41]. In TARF, a routing protocol is designed to prevent an attack that takes advantage of replaying routing information like Wormhole attack, Sinkhole attack, and Sybil attack. Here, a neighbour is defined as a node that is at a distance of one hop. Each node would have a neighbourhood table to accumulate energy cost and trust value for their neighbors and two elements run on every node that are EnergyWatcher and TrustManager. Energy cost, E_{Nb} is described as average energy consumed in delivering a packet successfully to BS and for this each node shares its energy cost report with its neighbours and its equation is given by relation: $E_{Nb} = E_{n\rightarrow b} + E_b$, where, $E_{n\rightarrow b}$ is cost in delivering a packet to one hop neighbour and E_b is energy cost received from neighbors that is energy cost for packet delivery to BS. A compromised node may generate a false energy report in order to lure all traffic. In that case, there is TrustManager that decide trust level of

each neighbour by finding any network loops and inappropriate data delivery. For detecting loops, forwarded sequence interval will be examined and if received data packet matches with previously recorded entry then TrustManager will demote trust value and delivery ratio will be decided by number of successfully delivered packets.

With a similar motive of secure routing A Trust-Aware Secure Routing Framework in WSNs is proposed by Duan Junqi et al. [42]. A light weight model is presented to resist various attacks. For calculating trust of node j for node i which is also used in [50]:

$$t(i,j)^l = \alpha \times dt(i,j)^l + \beta \times \frac{\sum_{(k \epsilon C_j, k \neq i)}^{n} it(k,j)^l}{n-1}$$

Where dt (i,j) is for calculating direct trust and second term represent recommendation from node k. Indirect trust is calculated by utilizing theory of semirings [43, 44]. Factors α and β are introduced in order to resist conflicting behaviour attack. Larger value of α suggests that node is more relying on itself and high value of β represents that recommenders are trustworthy. While calculating direct trust another factor γ is used to deal with on-off attacks which will handle whether past interaction will be given preference or current values are more important. An intrusion detection system is also attached with each node and its result will be used by direct trust to analyze positive and negative assessment. To handle bad mouthing attack and collusion attack an inconsistency check scheme is also proposed in this system. In addition, by using these trust results a secure routing path is taken to safely deliver packets.

Compared to TSRF, Rajaram et al. proposed a Secure Routing Path Using Trust Values for WSNs model [45] which concentrates more on indirect trust. In addition this scheme focuses on mobility of nodes, When a node is constantly moving it would be not advisable to calculate direct trust for that node every time as this will consume more time as well as energy. In this case it is beneficial to take recommendations from other nodes. For assigning trust values, every node monitors its neighbour's node and analyse its packet delivery efficiency that is how much packets node is forwarding that it receives and if PDR is high a higher trust value that approaches to 1 will be assigned, while 0 value concludes malign activity. The node that drops minimum number of packets will be chosen as next node for secure routing.

Another distributed approach, called Trust Management Scheme Based on D-S Evidence Theory for WSNs is proposed by Feng et al. in [46]. This scheme has concentrated on trust characteristics namely transitivity, subjectivity and uncertainty. Like other reputation based

model, trust is calculated based upon direct observation and recommendation from other nodes. Direct trust is calculated by following expression:

$$DT_{i,j} = \beta \times HDT_{i,j} + (1 - \beta) \times CDT_{i,j}$$

Where $HDT_{i,j}$and $CDT_{i,j}$is history observations and current observations of node i for node j respectively and β is a factor to prevent on-off attack which assign weights to both observations. However if node i has no source for direct observation on node j then it will consider recommendations from common neighbors of node i as well as node j. Indirect trust is given by $RT_{i,j} = DT_{i,k} \otimes DT_{k,j}$. $RT_{i,j}$ will only be considered trusted if both $DT_{i,k}$ and $DT_{k,j}$ are trusted and this way trust transitivity characteristic property can be maintained. For aggregating recommendations, a factor I_u is used to assign weights to different recommendations and these weights will be retrieved by revised Dempster-Shafer evidence theory. Difference of two recommendations is calculated and if it is inconsistent, there are chances of false recommendations. Thus by analysing consistency bad mouthing attack can be defeated.

A dynamic trust model exploiting the time slice in WSNs is presented in [47]. G. Wu et al. introduced a scheme where Time slices are used to identify pseudo malicious nodes that are nodes behaving abnormally because of some accepted reasons like link breakage, signal interventions. Those nodes should be given another chance within that time slice to prove their trustworthiness. The model include four phases: first phase is for observing trust through direct as well as indirect information based upon selected trust metrics, second phase include calculating trust values based on fuzzy logic [48], third phase includes choosing most trusted neighbour to forward packet and this is done by using grey theory [49] which is used with system having lack of information, and final phase is recovery stage based on time slices to detect pseudo-selfish nodes where these nodes can be turned into trusted node.

Another trust model for detection of malicious nodes has been proposed by J. Jiang et al. [54]. Here an energy efficient distributed trust model (EDTM) has been proposed. It contains two important components that are multihop trust model and single hop trust model. If entry of object node is present in list of neighbouring nodes then subject node triggers single hop trust model otherwise multihop trust model is selected. In first step by analyzing number of packets fetched by sensor nodes, direct trust and indirect trust are determined. After that energy trust, data trust and communication trust are used for determination of direct trust. Advantage of this protocol is that it can be used data fusion, trusted key exchange. In addition

EDTM can be used for enhancing security in routing. Memory requirement and energy requirement are less for this protocol.

With a similar motive of secure routing Energy-Efficient Trust System Through Watchdog Optimization has been proposed by P. Zhou et al. [55]. In this paper main focus is optimisation of watchdog mechanism by minimising cost of energy in usage. Both Inside attacks and outside attacks are considered for this approach. Three main concepts are introduced in this scheme i.e. trustworthiness for determining sensor node behaviour and trust robustness and trust accuracy for measuring how exactly object node trustworthiness can be gained in presence of attacks of WSNs. Trust accuracy and trust robustness need not to be calculated at run time. Two algorithms that are Distance-Based Probabilistic (DBP) Algorithm and Heuristic Watchdog Frequency Adjustment (HWFA) Algorithm are proposed in this scheme. The approach is helpful in providing resistance against bad- mouthing attack, on-off attack and discrimination attack. This type of research could be extended in future to optimize watchdog mechanism.

A comparison of above discussed scheme is being presented in table 2.1 and table 2.2. Factors considered for comparison includes methodology used to calculate trust, trust architecture, source of trust i.e. direct or indirect trust, trust attributes, protocols used in routing by trust models, simulation platform, merits and demerits of proposed scheme.

Table 2.1: Cluster-based WSNs trust models

Scheme	Methodology	Trust architecture	Source of trust	Trust attributes	Protocol used for routing	Simulations	Merits	Demerits
HTMS [30]	Weighting; Probability theory based on SPN	HYB	DT, IT	QoS, Social	HEED	Real world	Considered social trust along with qos trust	Computational overhead is high
TLEACH [32]	Probability theory; beta distribution	DIS	DT, IT	Situational trust	LEACH	Omnet++	CH chosen cannot be malicious	Energy and communication overhead is high
LEACH-TM[34]	Weighting; Probability theory		DT, IT	Energy	LEACH	Ns2	Suitable for large network	Results of this model are not presented
HATWA [25]	Heuristic	HYB	DT, IT	Security, mobility, Reliability	---------	Ns2	Calculated trust for group of nodes rather than	Dependency on n/w monitoring module

							single node	
LWDTM [36]	Beta probability density function; matrix theory	HYB	DT, IT	Data values comparisons, cooperation.	LEACH	Ns3	Light weight model no overhead	CH security is not taken into account
FBTM [37]	Fuzzy Logic	CEN	DT	Packet transmission rate, PDR	AODV	--------	Fuzzy is good technique for aggregation, thus reducing computational overhead	Results of this model are yet to come
FBTARF [38]	Fuzzy Logic	DIS	DT	Energy, Distance	---------	Ns2	PDR, throughput is improved	Memory requirements are high
FTPR [39]	Fuzzy Logic	HYB	DT,IT		-------	Ns2	Communication overhead is less	It is assumed that nodes have special id which is not acceptable for various applications

Table 2.2: Flat WSNs trust models

Scheme	Methodology	Trust architecture	Source of trust	Trust attributes	Protocol used for routing	Simulation	Merits	Demerits
TARF [41]	Weighting; Probability theory	DIS	DT	QoS (Discovery of network loop, delivery ratio)	TARF	MOTELAB	Prevent replay attack, no stringent time synchronisation required	TrustManager demotes trust of a legitimate node, if attack is occurring on a successor node connected to honest node
TSRF [42]	Weighted; semirings theory	DIS	DT, IT	QoS	TSRF	Ns2	Considered multihop routing	Do not considered mobility of nodes

TMFL [40]	Fuzzy logic	CEN	IT	Not mentioned	---------	C language	Fuzzy logic can reduce time and computational overhead	Bottleneck on centralized node and no attack analysis
SRPUTV [45]	Weighted	DIS	DT, IT	QoS (Packet delivery).	Link state routing	MATLAB	By choosing correct path, packet can be transmitted successfully	Do not consider how to update trust values
TMSBDS [46]	Dempster Shafer theory	DIS	DT,IT	QoS (Received packet rate, successfully sending packet rate, packet forwarding rate, node availability)	---------	MATLAB	Energy requirements are low	Store computation is high and thus not suitable for highly dense network
DTMETS [47]	Fuzzy logic and Grey Theory.	DIS	DT,IT	QoS and General (Energy, packet loss rate, successful interaction, success rate of exchange)	---------	NS2	Pseudo-selfish node can be recovered	Attack analysis is not considered
EDTM [54]	Weighted Theory, Ray Projection Method	DIS	DT, IT	QoS (PDR, Energy)	----------	MATLAB	Energy and memory requirements are less	Defining threshold and weight is still an issue

DT: Direct trust, IT: Indirect trust; HYB: Hybrid, CEN: Centralized, DIS: Distributed

2.5 Attack analysis on Trust based scheme

In this section a comparison of those above mentioned schemes with respect to its ability to provide prevention against malicious attacks is made. The models which are resilient towards

any specific kinds of attacks are marked with ✓ symbol and × represent not successful holding. The models which have capacity to prevent against malicious attacks are being compared rest other models doesn't provide prevention against any attack and comparison is provided in table 2.3.

Table 2.3: Attack analysis

Scheme	Sinkhole	Sybil	Bad-mouthing	DoS	On-off	Greyhole	Black hole	Wormhole	Conflicting behaviour
HTMS [30]	✓	×	✓	×	✓	×	✓	×	×
TLEACH [21]	×	×	✓	×	✓	×	×	×	×
LEACH-TM[32]	×	×	×	×	✓	×	×	✓	×
HATWA [25]	×	×	×	×	×	×	×	×	×
LWDTM [36]	×	×	×	×	×	×	×	×	×
TARF [41]	×	✓	×	×	✓	×	✓	✓	✓
TSRF [42]	×	×	✓	×	✓	✓	×	×	✓
SRPUTV [45]	×	×	✓	×	✓	×	×	×	×
TMSBDS [46]	×	×	✓	×	✓	×	×	×	×
FTPR [39]	×	×	×	×	✓	×	✓	×	✓
EDTM [54]	×	×	×	×	✓	✓	×	×	×
ETWO [55]	×	×	✓	×	✓	×	×	×	×

CHAPTER 3

PROBLEM STATEMENT

WSNs are placed in open environment. Hence it is easy for an attacker to compromise such network easily. In cluster-based approach nodes send data to its CH which further route data to BS. However, compromised cluster-head may behave maliciously which may lead to packet drop, poor network performance. In certain applications such as health monitoring, battlefield it is necessary to safely route data. Researchers are doing focus on finding security solution for WSNs. A cryptographic solution requires high computational capacity, power and resource. As sensor networks are open and dynamic in nature. So it is easy for an adversary to compromise network and steal keys, thus making network an unsecure network. Hence trust can be incorporated with WSNs to make it more secure. The aim of a trust based routing protocol is to find out secure path by selecting trusted cluster-head i.e. cluster-head with low trust value should not be included in routing for final delivery of data to BS.

Leach is one of the clustering-based approach used for routing purpose, but there are many problems associated with LEACH one of the problem is finding trusted cluster-head. Security is not considered while designing LEACH protocol, thus sensor networks are prone to many attacks such as DoS attack, Sybil attack, Blackhole attack, Sinkhole attack etc. In addition calculation of trust method should be energy efficient as sensor networks have limited source of charging. Thus protocol designed should be secure and energy efficient.

3.1 Objectives

The main goal is to provide an energy efficient solution to enhance security by means of trust management. To accomplish the goal following objectives are considered:

- To study and simulate LEACH protocol in MATLAB.
- To analyze limitations in LEACH.
- To study different trust schemes available in literature for enhancing security.
- To embed some malicious nodes in network and analyze performance degradation caused by them.
- To design energy efficient and trust aware routing algorithm in LEACH that will consider remaining energy, PDR and distance to calculate trust.
- To implement the above algorithm in MATLAB and compare it with normal LEACH using performance metrics such as network lifetime, PDR, trust evolution.

CHAPTER 4

SIMULATOR INTRODUCTION (MATLAB)

4.1 Simulator Introduction

MATLAB [51] is high level language provided with toolboxes and commands to make it comfortable for user to use inbuilt functions. MATLAB which is acronym for matrix laboratory is a fourth generation language. MATLAB has certain capabilities like numeric computation, data analysis and visualization, programming and algorithm development, application development and deployment, performing numerical computation. It is possible to import data into MATLAB from files or other applications or any other external source, once data is imported into MATLAB environment. It could be easily analyzed through built-in engineering functions. In addition different types of graphs can be plotted through MATLAB in-built functionality. MATLAB supports simple vectors and matrix operations that are fundamental to engineering and scientific problems. MATLAB provides a huge library of mathematical functions for statistics and linear algebra. Commands can be executed one at a time providing immediate results. Moreover, MATLAB allows one to examine different approaches to obtain optimal results. MATLAB supports creating different scripts and function to reuse and automates work.

MATLAB has become popular language for technical computing. With the help of development tools in MATLAB one can implement their algorithm efficiently and optimize their performance. MATLAB also supports features of traditional programming language along with layout tools for composition of custom graphical user interface. Further functionality of MATLAB can be extended with add-on toolbox to solve problems in range of application including signal processing; image processing, computational biology, control systems etc. With the help of MATLAB it is possible to share work. MATLAB concluded results and codes can be published automatically. Applications and algorithm developed in MATLAB can be distributed as a stand-alone executables, components for merging in other software environments for example excel. C code can also be imported within MATLAB. One million people all over the world are taking advantage of MATLAB.

The main working window of MATLAB is known as Desktop. The layout of a desktop is shown below in figure 4.1. A desktop has further 4 panels:

- Current folder: With this panel one is able to access current folders and files of project

- Command window: It is prompted by >>. It is a place where user types in commands to be executed.
- Workspace: This panel has details about the variables created in the programs or may be imported from other programs.
- Command history: This panel has details about commands executed in past.

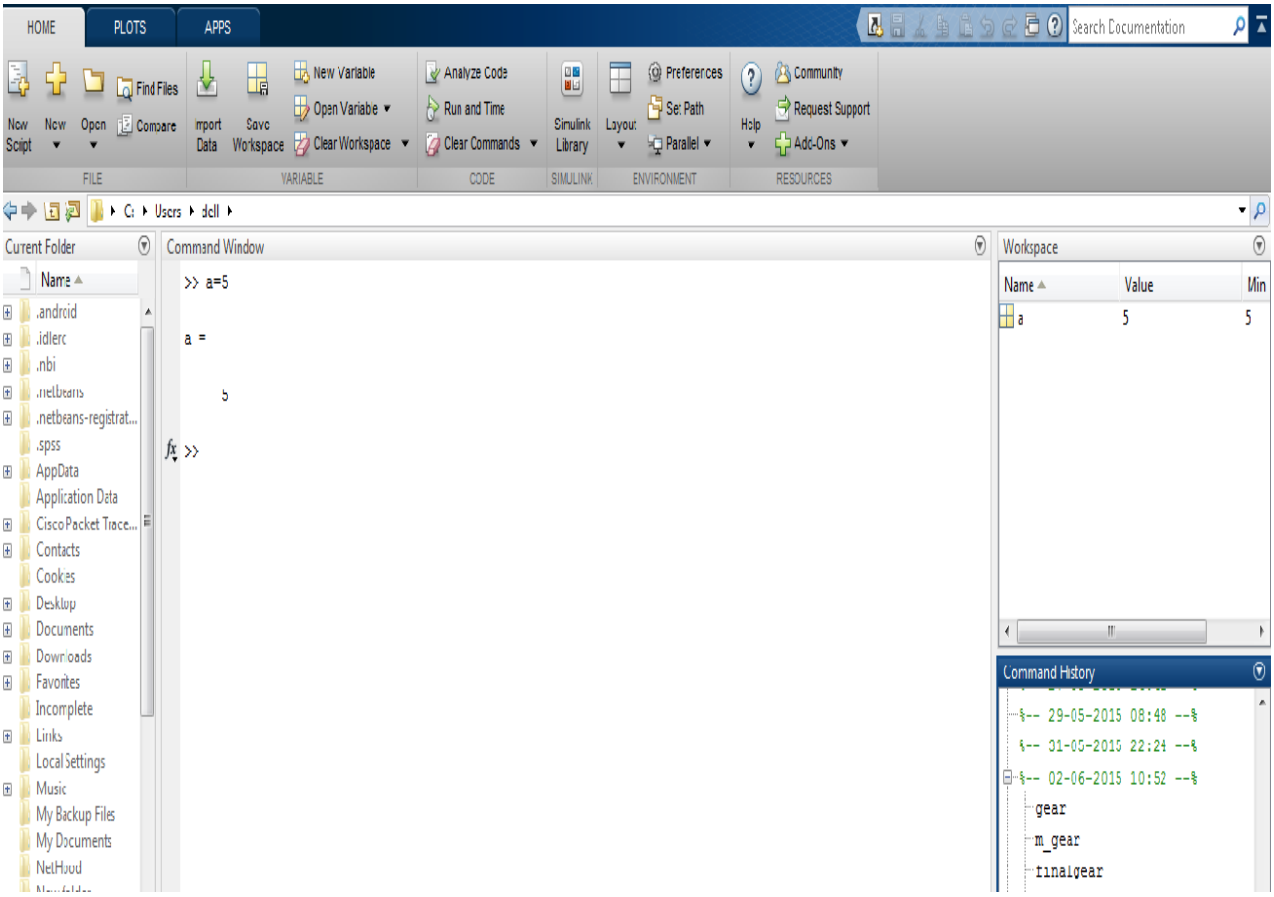

Figure 4.1: Desktop view of MATLAB

With MATLAB it is possible to create two types of programme files:

- Scripts: These are the program files saves with .m extension. Whatever commands written in script file is executed. Scripts neither take inputs from users nor return any output.
- 1Functions: Functions are also saved with .m extension. They are different from script in the way that functions can accept user input as well as they return some output.

MATLAB editor allows writing scripts or functions to be executed.

CHAPTER 5
PROPOSED ALGORITHM

LEACH [12] is clustering based approach where nodes arrange themselves into local area called clusters. After every round a new CH is selected to balance energy load. Every new round starts with Set-up phase proceeded by Steady-state phase. In Set-up phase clusters are formed based on some threshold value which is given by equation 5.1:

$$T(n) = \frac{p}{1-p\times r\ mod(1/p)} \quad (5.1)$$

After this sensor nodes will decide which CH to choose based on signal strength. Next based on strength of sensor in a cluster, CH will form a TDMA schedule and each node is supposed to transmit within their allotted slot. After collecting data from every cluster members, CH aggregates data and then sends data to BS.

But there are some problems associated with LEACH. Though CH selection procedure ensures that all nodes would get an equal chance to become CH but energy factor is not considered while selecting CH. After a time period, it is likely that a node with low energy may get selected as CH [52]. Another problem is that different CH elected would have different distance to BS, so their energy needs would also be different [53]. In addition, in large network that CH which is located at more distance from BS has to adopt multipath path which consumes high energy. Moreover, energy demands for intra cluster communication are less than inter cluster communication. LEACH is completely dependent on CH for transmission and aggregation of data and a compromised CH would drop packets and may not perform task assigned to it thus making an unsecure network. Thus it is very important to choose a trusted CH.

5.1 Assumptions

For executing trust mechanism for sensor networks environment, following assumptions have been made:

- There are some malicious nodes present in the network
- BS has unlimited source of energy and it is free from any kind of attack
- If a node is performing some malicious activity then it will be penalized and its trust value will decrease.

- If a node is showing good behaviour, it will be rewarded and its trust value will be increased.
- Malicious nodes present in network are consuming more energy and dropping more packets than normal nodes.

5.2 Proposed algorithm

Aim of this protocol is to choose trusted CH i.e. nodes with less trust value or less energy should not be selected as CH. Proposed work can be divide into two main modules that is trust based routing module and trust management module. Figure 5.1 represents overall architecture of proposed algorithm.

- **Trust Management module:** This module calculates trust based upon remaining energy, PDR and distance.
- **Trust-based routing module:** It is almost same as basic LEACH protocols with some changes in it. Trust-based routing module uses trust management module to perform secure routing.

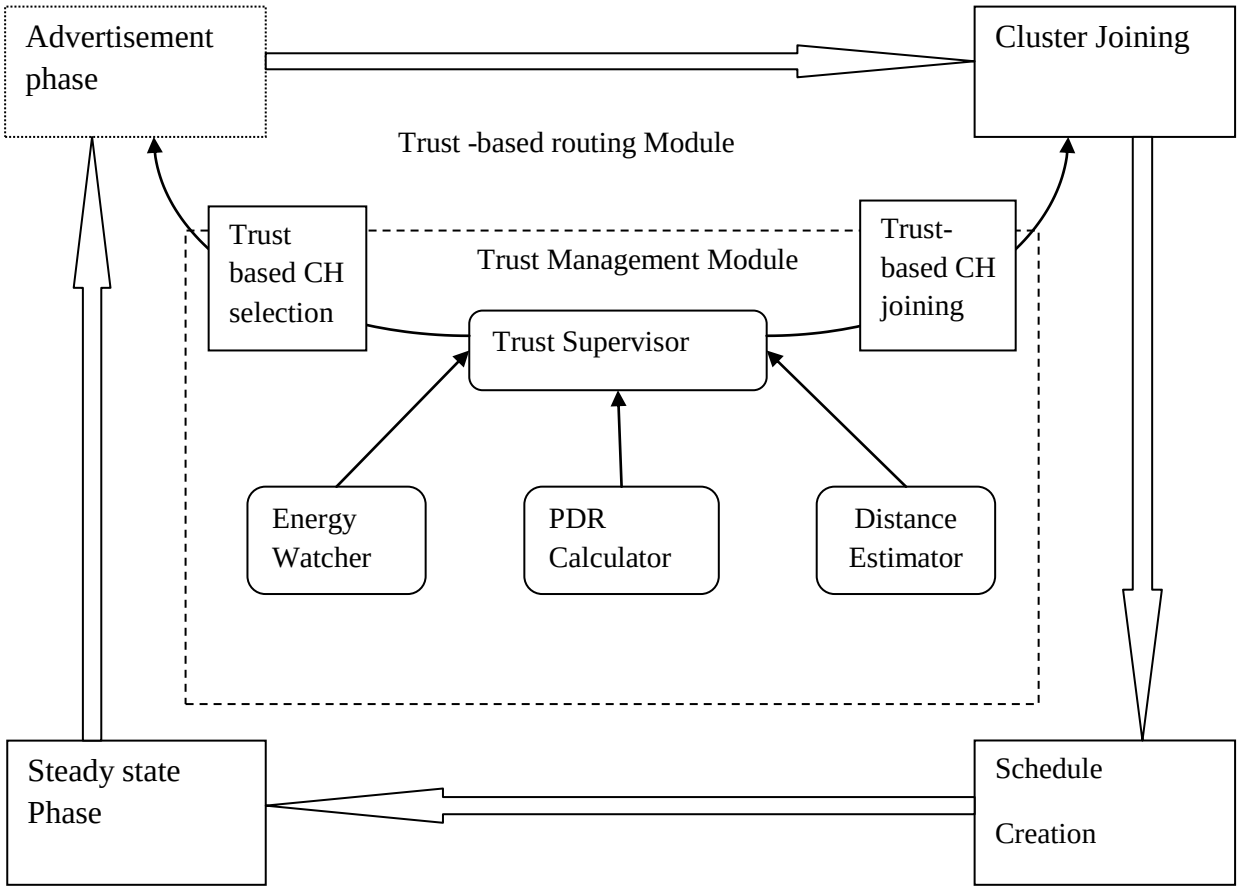

Figure 5.1: System Architecture

An improvement in LEACH protocol has been proposed, while maintaining the routing of original LEACH protocol. The scheme used to calculate trust is described below:

Inputs

- Network area
- Number of nodes

Nodes will be randomly distributed in given area. Every node runs with an energy watcher, PDR calculator, distance estimator and trust supervisor. Energy Watcher will calculate remaining energy of neighbour nodes and CHs, PDR calculator will calculate PDR of every node based upon number of packets dropped by node, Distance Manager will calculate and maintain distance between node and neighbours node along with CH distance with node Trust Supervisor will maintain trust level of neighbouring nodes and CHs elected by considering three factors that are remaining energy, PDR and distance between nodes. For calculating trust value three factors will be considered that are remaining energy, PDR and distance i.e. nodes with high remaining energy, high PDR, and less distance between nodes will have more trust value and thus have high chances of becoming CH as compared to those nodes with low trust value, low PDR and high distance between nodes. These four components will work as follows:

- **Energy Watcher**: It will keep track of remaining energy of nodes. Energy model for the network is discussed as: To transmit a k-bit message with a distance of d, energy consumption can be calculated by:

  $$E_t = E_e(k, d) + E_a(k, d) \quad (5.2)$$

  Where E_t is the transmitting energy, E_e is energy required to run transmitter and receiver circuitry, E_a is transmitter amplifier energy and energy required to receive any packet can be calculated by:

  $$E_r = k * E_e \quad (5.3)$$

  Hence energy will be consumed while transmitting or receiving packets in the network. As sensor networks are deployed in area where it is not possible to charge these nodes timely, so protocol designed should be energy efficient to save energy of these nodes and increasing network lifetime.
- **PDR Calculator**: This component will keep track of PDR. From the past records PDR calculator will maintain total number of packets sent to BS and how many of them are actually received by BS. Packets may be intentionally dropped by malicious node. Another reason for packets drop may be poor network connectivity. Node with

high PDR will have high trust value and node with low PDR will have less trust value. Formula for PDR can be given as:

$$\text{Packet\_Delivery\_Ratio} = \text{Packets\_Rcvd}/\text{Packets\_TO\_BS} \quad (5.4)$$

Where, Packets_Rcvd are total number of packets received by BS and Packets_TO_BS are total number of packets sent to BS.

- **Distance Estimator**: This component will keep track of distance between nodes. If distance between evaluated node and subject node is less, a high trust value will be assigned to evaluated node otherwise if distance between subject node and evaluated node is high, then low trust value will be assigned to node. Hence trust value is inversely proportional to distance between nodes. Also this component will keep track of distance between nodes and CH.
- **Trust Supervisor**: This component will maintain trust values of nodes that will be used by routing module for trusted CH election and secure routing. The working of trust supervisor is being discussed in trust management module.

5.2.1 Trust Management module

For calculating trust, trust supervisor will calculate both direct and indirect trust and final trust will be calculated by aggregating both trust values. Direct trust is that trust which is calculated by nodes itself. Direct trust will be calculated based on past and present interactions of nodes. Sometimes it is not possible for a node to calculate direct trust of other nodes in order to save energy; in that case nodes will take recommendations from other nodes which will result in indirect trust. Indirect trust is also called second hand trust. In this model trust is calculated by considering energy, distance and PDR as trust metric. Nodes with high remaining energy, high PDR, less distance between nodes will have more trust value as compared to those nodes with less remaining energy, less PDR, more distance between nodes. As shown in figure 5.2 a subject node is one which wants to calculate trust of other node, evaluated node is one whose trust value is to be calculated, recommendation nodes are those whose opinions are considered for calculating indirect trust.

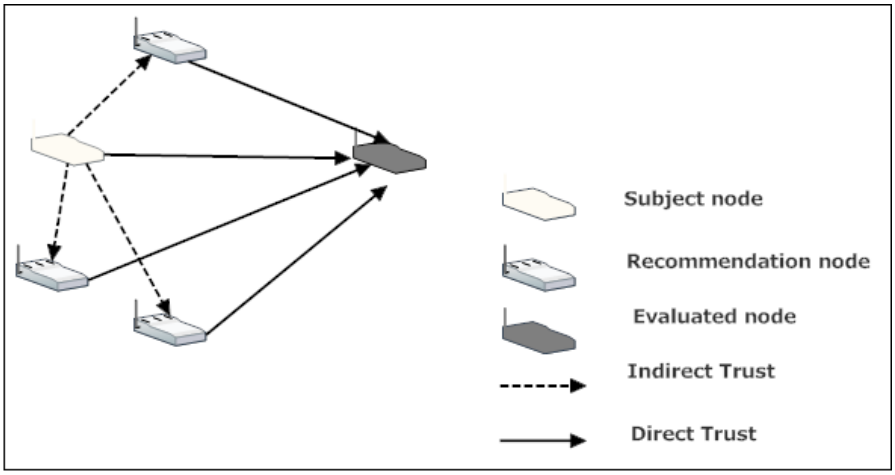

Figure 5.2: Trust Relationship

An initial trust of 0.5 is assigned to every node. For calculating direct trust, trust supervisor will interact with energy watcher, PDR calculator and distance estimator. For calculating direct trust, first trust supervisor will check remaining energy, and then a series of if-then rules will be applied to remaining energy, by comparing remaining energy with threshold value trust values will be assigned to nodes. Threshold values are selected by analyzing remaining energy after a particular round. Nodes will be awarded or penalized based upon the results after comparing remaining energy with threshold value. A node will be rewarded if its remaining energy is high after a particular round and if at the same round node is having less energy as compared to threshold then it will be penalized.

Once remaining energy has been checked, next trust supervisor will check PDR of nodes. PDR of nodes is compared with thresholds and then accordingly reward or penalty will be given. A node with high PDR will be rewarded and the nodes which drop more number of packets will have less PDR and hence penalized.

Further trust is dependent on another factor that is distance between nodes. If distance between nodes is high then corresponding trust of the node will be more and vice-versa. Hence direct trust can be calculated based upon aggregation of three factors.

Next, indirect trust will be calculated based on recommendations considered from other nodes. Indirect trust is the sum of trust values calculated by other nodes and given by equation 5.5:

$$IT_{A\to B}^{C} = \sum_{C} DT_{A\to C} \times DT_{C\to B} \quad (5.5)$$

Where, $IT_{A\to B}^{C}$ is indirect trust of B calculated by A considering recommendation from C and C≠ A; $DT_{A\to C}$ and $DT_{C\to B}$ are the direct trust value calculated by A for C and C for B.

For calculating final total trust both of direct and indirect trust will be aggregated as given below by 5.6:

$$TT_{A\to B} = wDT_{A\to B} + (1-w)IT_{A\to B}^{C} \quad (5.6)$$

$TT_{A\to B}$ is the total trust of node A on node B, w is the weight associated with direct and indirect trusts. A higher value of w signifies that sensor nodes relies more on its own judgement whereas a lower value of w signifies that sensor nodes has more trust on recommendations provided by other nodes. Final trust values of nodes will be stored by Trust Supervisor.

Trust_Calculation( )

Input: Remaining energy, Packet_delievery_ratio, Distance between nodes

1. Every node is assigned with initial direct trust of 0.5
2. if (R.E > Th_1)
3. DT= DT+ 5%of DT //node will be rewarded
4. elseif (Th_2<R.E < Th1)
5. DT=DT //trust will remain same
6. elseif (R.E<Th_2)
7. DT=DT-5%of DT //node will be penalized
8. end
9. if (PDR>Th_3)
10. DT=DT+5% of DT //node will be rewarded
11. elseif (Th_4<PDR<Th_3)
12. DT=DT //trust will remain same
13. elseif (PDR<Th_4)
14. DT= DT-5%of DT //node will be penalized
15. end
16. if ($D_{S.N \rightarrow E.N}$>Th_5)
17. DT=DT+5% of DT //node will be rewarded
18. elseif (Th_6<$D_{S.N \rightarrow E.N}$<Th_5)
19. DT=DT //trust will remain same
20. elseif ($D_{S.N \rightarrow E.N}$<$Th_{6.}$)
21. DT= DT-5%of DT //node will be penalized
22. end
23. Indirect trust will be calculated from recommendation nodes.
24. TT= w *DT + (1-w)*IT

Notations: DT= Direct Trust
IT= Indirect Trust
TT= Total Trust
Th= Threshold Value
$D_{S.N \rightarrow E.N}$= Distance between subject node and evaluated node

Figure 5.3: Pseudo Code for Trust_Calculation( ) in EETA-LEACH

5.2.2 Trust-based Routing module

Routing module consists of two main phases: Set-up phase and Steady-state phase. In Set-up phase clusters are arranged and selected followed by steady-state phase where nodes will transmit data to BS.

1. Set-up phase

a) Advertisement phase

This phase is same as in original LEACH protocol but for increasing lifetime of network energy factor is considered while selecting CH, so that the nodes with less energy should not get selected as CH. The number of nodes elected as CH with low energy will be less thus increasing network lifetime. To start procedure of CH election, node will select a random number between 0-1. If the number chosen is less than threshold node, node will be selected as CH otherwise not. The threshold value can be given by equation 5.7:

$$T(n) = \frac{p}{1-p\times r\ mod(1/p)} \frac{E_{REM}}{E_{INT}}, \quad n \epsilon G \tag{5.7}$$

Where p is the desired percentage of CHs, G is set of nodes that have not been elected as cluster-heads in the last 1/p rounds and r is the current round, E_{rem} is remaining energy of node and E_{int} is initial energy of node. After this phase, nodes has list of all eligible CH members.

Trusted CH arranging procedure

After CH has been selected, now elected CH will find all its CH neighbours and all information regarding CH neighbour will be collected from energy watcher, trust supervisor and distance manager. CH will maintain information of neighbour CH in form of a table. Each node will maintain an entry corresponding to every attribute mentioned in table 5.1.

Table 5.1: Neighbour CH Information

Attribute	**Description**
ID	ID of neighbouring CH
E_{REM}	Remaining energy of CH
T_{node}	Final trust of neighbouring CH
D_{Bs}	Minimum distance of neighbouring CH from BS
EC	How many times Neighbouring CH is elected as CH
$N_{nearest}$	Whether nearest neighbour or not

Now CH will examine whether neighbour is nearest neighbour or not and this will be decided by comparing distance of nodes with D. Equation 5.8 gives the value of D. Distance between CHs will be calculated with signal strength. If distance calculated is less than D then $N_{nearest} = 1\ else\ it\ is\ 0$.

$$D = \acute{\alpha}\ \times \sqrt{\frac{1}{\pi K}} \times L \tag{5.8}$$

Where L is the side length of the square area where sensor nodes are deployed, K is the number of cluster-heads; $\acute{\alpha}$ is an adjusting factor. This will uniformly cover whole area CHs.
If number of nearest neighbour CH is greater than 0 then CH will calculate trust weight associated with every nearest neighbour CH and trust weight, W_T is calculated by equation 5.9.

$$W_T = \alpha \times \frac{E_{REM}}{E_{INT}} + \beta \times \frac{T_{node}}{\sum T_{node}} + \gamma \times \frac{d(CH,BS)}{AD_{c\rightarrow BS}} + EC \tag{5.9}$$

Where, α, γ, β are the weight factors selected accordingly. As for this thesis energy is already considered as attribute for trust calculation, so for simulation a lower value of α is considered. If some other attribute is selected then a higher value for α should be considered otherwise β can have higher value as trust value already considered energy factor and EC is number of times node is selected as CH. T_{node} is the trust value of neighbouring CH obtained from trust management module. $\sum T_{node}$ is aggregation of trust of all nearest neighbour CH. CH with heaviest trust weight value is selected as new CH and will broadcast this information to other nodes and CH selected earlier will vanish. In addition, minimum distance of node from BS is also considered. CH distance to BS is compared with others nodes CH distance to BS and if difference between CH and BS is greater than predefined value, node will not be selected as CH. $d(CH, BS)$ is distance calculated between CH and BS and $AD_{c\rightarrow BS}$ is the acceptable distance between CH and BS. Hence CH selected with this procedure will be trusted, with better energy and will help in saving energy as transmitting energy cost will be less.

b) Cluster joining

In original protocol non-CH nodes join cluster based on signal strength received from CH but here nodes will select their CH based on trust values of cluster nodes.

c) Schedule Creation

CH receives all messages from nodes that would like to join cluster. Based upon strength of nodes in the cluster, CH begins to create a TDMA schedule and assign slots to non-cluster nodes to send data as well as to calculate trust.

2. Steady state phase

In steady state phase nodes will transmit sensed data to CH along with calculating trust. This phase can be divided into two slots data slots and trust slots [32] as shown in figure. After this phase every other round begins with set-up phase.

- **Data Slots:** Nodes will keep their transmitter on during their time slot only and will sense the data in the same time slot and send sensed data to CH selected meanwhile other nodes transmitters are off in order to save energy. It is assumed that CHs are having more energy than normal nodes so they keep their receivers always on to receive data from non-CH nodes.
- **Trust slots:** During this slot trust supervisor will calculate trust associated with their neighbors based upon considered factors as well as CH. Nodes update trust value regularly. In addition, CH will calculate trust of neighbour CHs in this slot and updates their table.

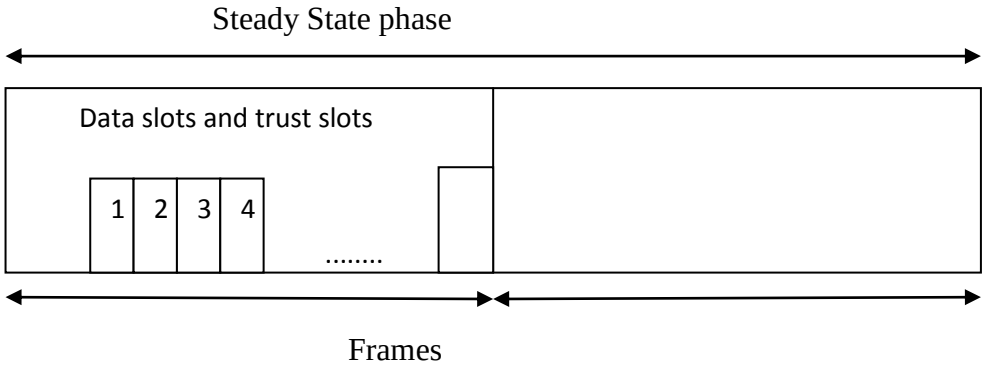

Figure 5.4: TDMA Schedule

For communication within a cluster i.e. an intra-cluster communication, amplification energy must be less than a inter-cluster communication that is a communication between CH and BS [53]. The reason behind this is within a cluster distance between nodes is less, so less of energy is needed to transmit a message as compared to inter-cluster communication. Therefore more energy could be saved.

1. Nodes will be randomly placed in an area.
2. for r=1:1:n
3. for i=1:1:n
4. temp__rand =rand // a random value between 0-1 well be chosen
5. if (temp_rand <=((p/(1-p*mod(r, round(1/p))* E_{rem}/E_{int}))))
6. Then CH will be selected
7. Total_trust=Trust_Calculation( ) // nodes will calculate trust of other nodes
8. CH will find its close neighbour
9. D=phi*sqrt(1/pi/K)*L;
10. if ((distance between CH and close neighbour CH)<D)
11. then N_{close}=True
12. else N_{close}=False
13. N=count number of close CH neighbour
14. if (N>0)
15. Then Compute weight of each close neighbour
16. $W_T = \alpha \times \frac{E_{REM}}{E_{INT}} + \beta \times \frac{T_{node}}{\sum T_{node}} + \gamma \times \frac{d(CH,BS)}{AD_{c \to BS}} + EC$
17. Node with heaviest weight factor will be selected as trusted CH
18. Nodes will join the CH with maximum weight value

Notations: r= Number of rounds
n= Total number of nodes

Figure 5.5: Pseudo Code for Routing Module in EETA-LEACH

CHAPTER 6

SIMULATION RESULTS AND DISCUSSION

The proposed algorithm EETA-LEACH has been designed in MATLAB [51]. It is considered that 100 nodes are randomly distributed over area of 100×100 m^2. Firstly basic LEACH is implemented. Sensor nodes send data to CH, CH after aggregating the data from cluster members further route it to BS. To study better results of trust management scheme some malicious nodes are introduced in network. It is assumed that malicious nodes are consuming high energy and dropping packets. It may be possible that selected CH is malicious which will drop packets that were supposed to send to BS i.e. malicious nodes defined in the network are launching selective forwarding attack. After implementing trust management scheme, chances of selecting malicious CH is almost negligible which will enhance network performance. Hence, proposed scheme is energy efficient, so network lifetime is improved with this scheme. In addition CH with heaviest trust weight is selected, so probability of packets drop ratio is decreased.

Evaluation is done based upon following metrics:

- Network lifetime
- PDR

Simulator parameters are mentioned in table 6.1.

Table 6.1: Simulation Parameters

Network parameters	**Values**
Network Size	$100X100m^2$
Number of nodes	100
Packet Size	4000 bits
Routing Protocol	LEACH
Initial battery power of node	0.5 J/node
Energy to run transmitter and receiver	50 nJ/bit
Data aggregation energy	5 nJ/bit
Amplification Energy (Cluster to BS)	$Efs = 10pJ/bit/m^2$
Amplification Energy (Intra Cluster Comm.)	$Efs/10 = Efs_1$

6.1 Simulation Results

Selection of CH

Figure 6.1 shows random distribution of sensor nodes in an area of 100*100 sq. units and LEACH protocol is simulated for routing purpose. There are some malicious nodes present in the network. Malicious nodes are represented by a plus (+) sign, normal nodes are represented with a circle (o). In addition selection of CH in particular round is also presented in figure 6.1. Nodes that are selected as CH are represented with dark blue asterisk. It can be easily analyzed that if no security practises are adopted, malicious nodes present in network could be selected as CH. Hence as a result malicious CH selected would drop packets received from cluster members which in result reduce network performance.

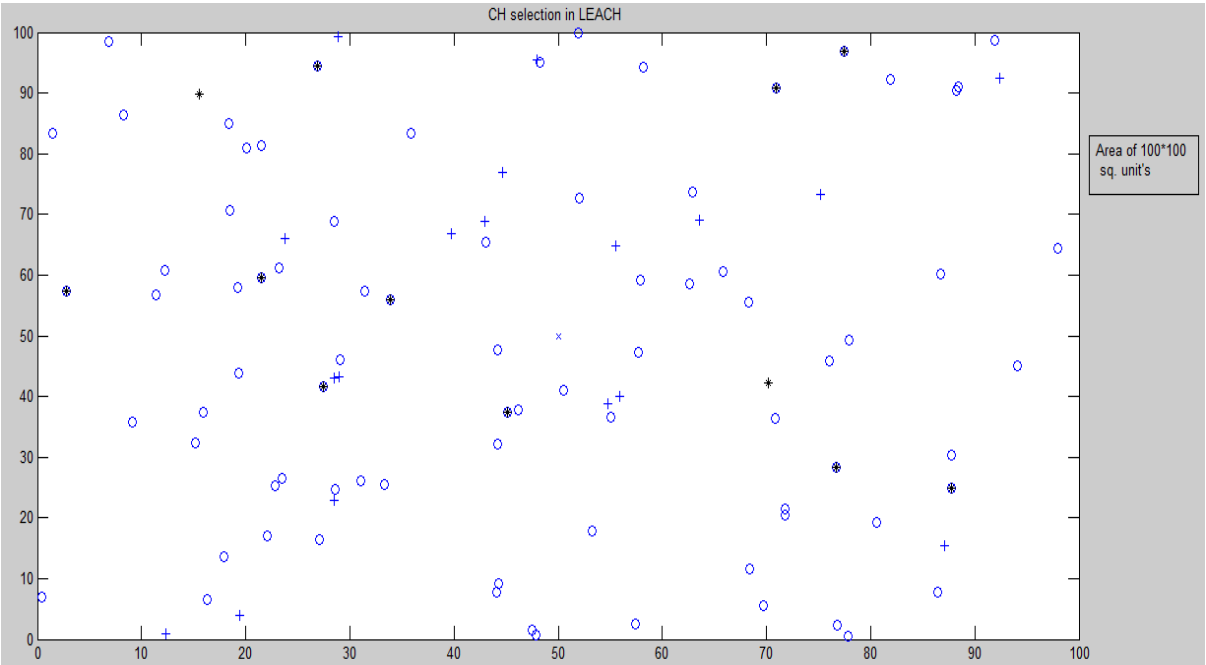

Figure 6.1: CH selection in LEACH

After implementing EETA-LEACH, it is verified that chances of selecting malicious nodes as CH are almost negligible. In EETA-LEACH, CH is selected based upon trust values of nodes. Therefore selected CH will not be malicious. The whole scenario is represented in figure 6.2. Trusted CH selected is represented by Green asterisk.

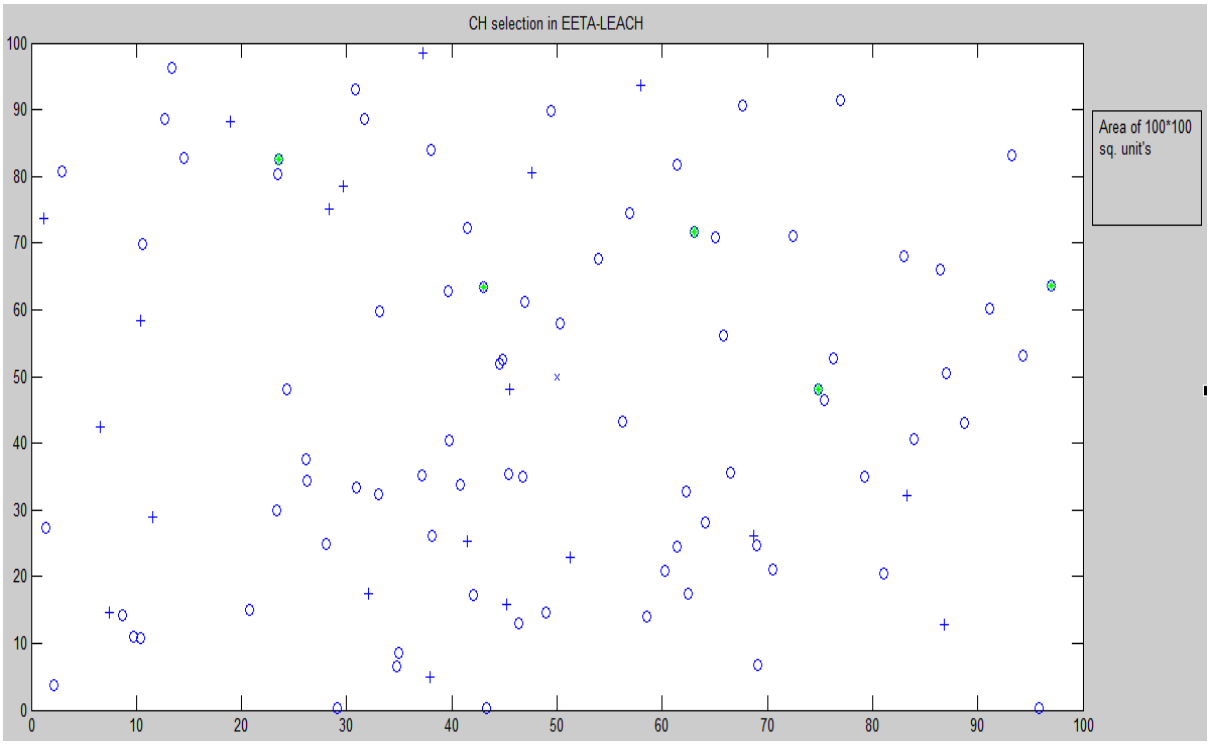

Figure 6.2: CH selection in EETA-LEACH

Trust Evolution

Figure 6.3 plots trust value of a malicious node. Trust value of a malicious node decreases as time increases. The value of $_W$ is selected chosen to be 0.5 in equation 5.6 which concludes that node is equally considering direct trust as well as recommended trust and value of α, β, γ are selected to be 0.2, 0.6, 0.2 in equation 5.9.

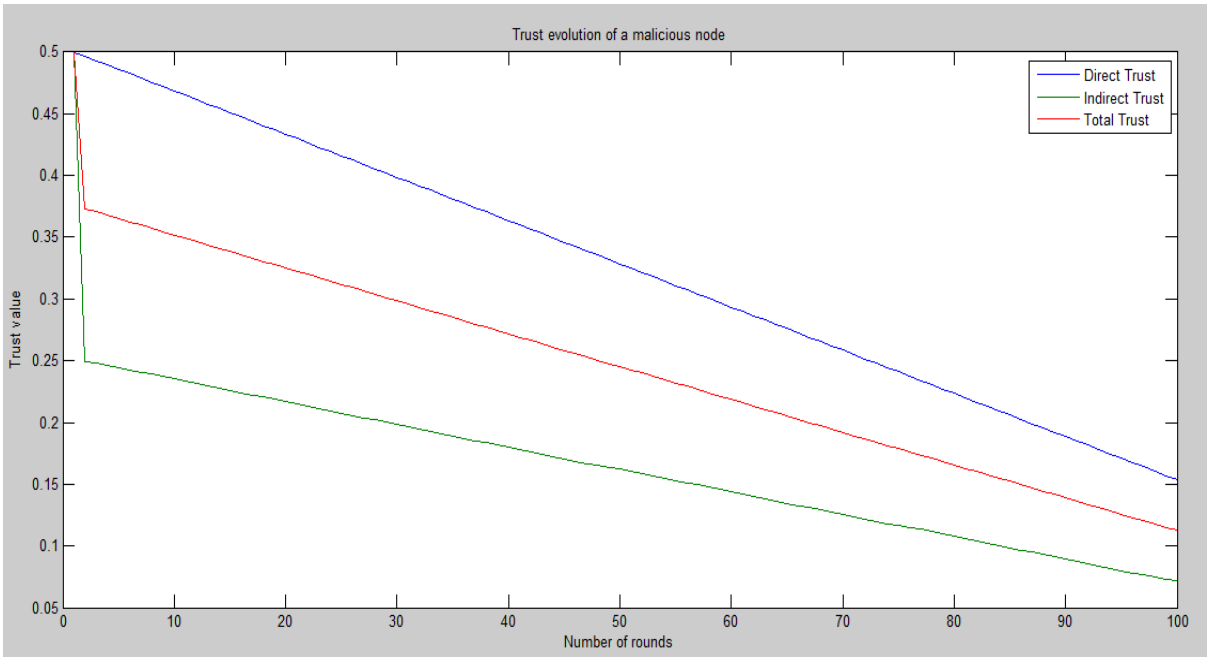

Figure 6.3: Trust evolution of a malicious node

At very first round node will have direct trust of 0.5, no indirect trust will be considered at first round, hence total trust will constitute to 0.5. Similarly at 10^{th} round direct trust is 0.4800, indirect trust is 0.2438 and thus total trust is 0.3619 for this round. In the proposed model calculated trust is directly proportional to remaining energy and PDR, as malicious node consumes more energy, drops more packets therefore its trust value decreases as number of round increases.

Analysis of PDR

Figure 6.4 shows number of malicious node versus average PDR. It could be observed that average PDR is 96% in EETA-LEACH and 91% in LEACH when there is no malicious node present in the network. There would be some packet loss because of poor network connectivity. Therefore PDR would not be 100% even if no malicious node present in the network. With presence of 5 malicious nodes in network EETA-LEACH network has PDR value of 0.9400 and LEACH has 0.8390, hence after implementing EETA-LEACH PDR increases by 12%. Similarly when 15 malicious nodes are present PDR is increased by 14% and with presence of 25 malicious nodes PDR increases by 21.5%. Hence it could be concluded that after implementing EETA-LEACH average PDR ratio is increased by 15.8%. EETA-LEACH has high average PDR as compared to leach because malicious nodes are not selected as CH and hence there are less packet drop in the network. Moreover EETA-LEACH can help in avoiding selective forwarding attack.

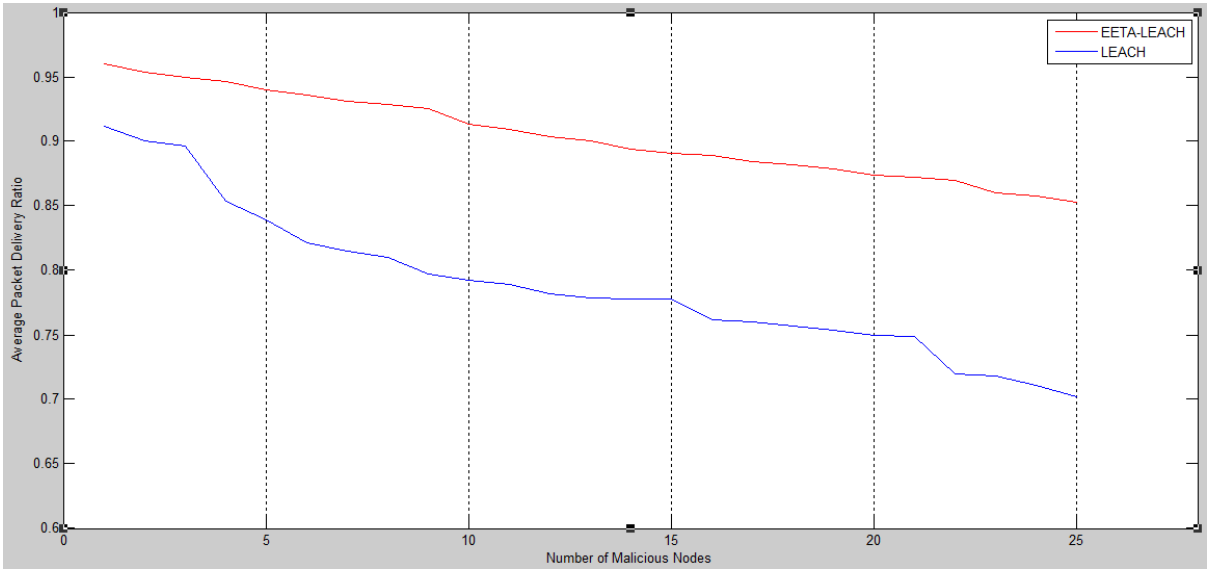

Figure 6.4: PDR versus number of malicious node

Network lifetime comparison

While comparing network lifetime it has been observed that EETA-LEACH has better lifetime as compared to LEACH. As in LEACH there are many retransmissions as compared to EETA-LEACH, in addition in EETA-LEACH less of malicious nodes would be selected as CH so less consumption of energy as it is assumed that malicious nodes are consuming more energy. Moreover, consumption of less energy while intra-cluster communication as compared to inter-cluster communication and consideration of energy factor while selecting CH makes EETA-LEACH more energy efficient. It could be verified from figure that in LEACH first node dies near 700th rounds as compared to EETA-LEACH where first node dies at 1100th round. Figure 6.5 shows network lifetime comparison.

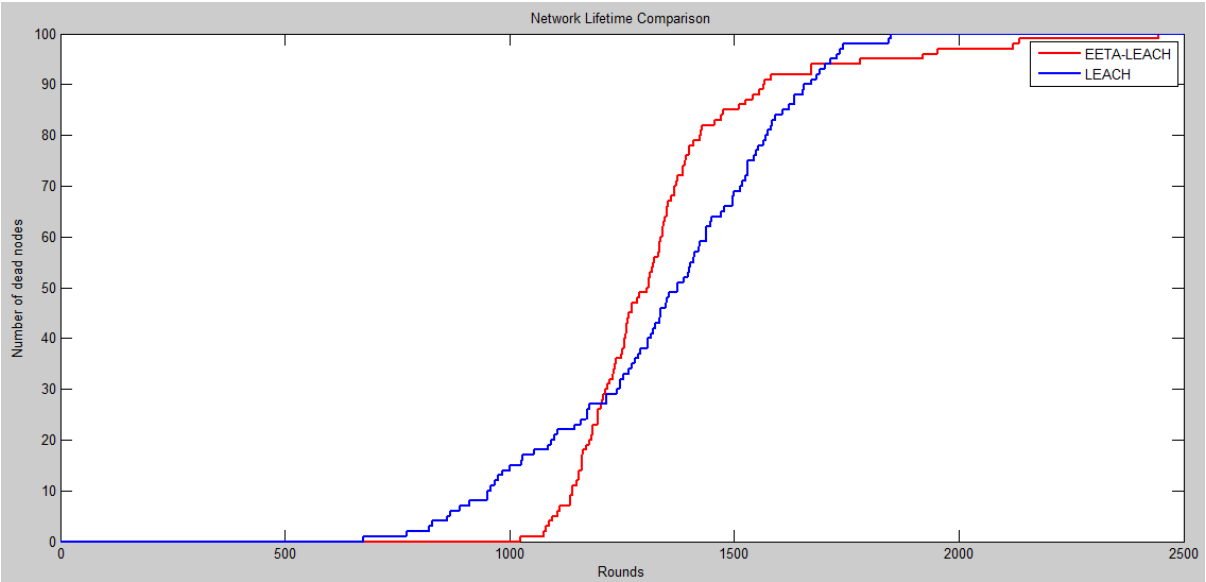

Figure 6.5: Network Lifetime Comparison

CHAPTER 7
CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

In this paper an energy efficient trust based approach has been proposed which is combination of trust-based routing module and trust management module. In trust management module, trust supervisor calculates trust for nodes as well CH that can be used for trusted CH selection and secure routing. Total trust value is a combination of direct trust that is calculated by node itself and indirect trust which is trust from recommendation nodes. Trust-based routing module modifies original LEACH. Routing module comprises of further four phases that are advertisement phase, cluster joining, schedule creation and steady state phase. Nodes that are malicious in nature will have less PDR and consumes more energy. So these malicious nodes will not be selected as CH because their computed trust value will be less. In addition, routing module uses less energy for intra-cluster communication as compared to inter-cluster communication which would help in improving network lifetime.

Protocol performance is verified using MATLAB simulator. It is verified that malicious nodes will not be selected as CH and trust value of a malicious node decreases with time. Simulation results proved that proposed algorithm consumes less energy and improves PDR as there are less number of retransmission. Average PDR is improved by 15.8%. In addition with implementation of EETA-LEACH, network lifetime improves as first node dies at 1100^{th} round in EETA-LEACH as compared to LEACH where first node dies at 700^{th} round.

7.2 Future Scope

In future, this work could be extended by considering other types of WSNs e.g. dynamic WSNs, heterogeneous WSNs. Other social trust attributes such as privacy, intimacy, number of interaction could be considered in future to extend this work. Beside this trust model could be further extended to develop lightweight algorithm to further reduce energy consumption. Memory requirement for this protocol are bit high as past records has to be stored by energy watcher, trust supervisor, PDR calculator. So challenging problem is to reduce memory requirements. In this thesis, nodes that have less PDR are considered as malicious without considering the fact that less PDR could be less because of poor network connectivity, this also motivates future wok**.**

REFERENCES

[1] M. Lucchi, A. Giorgetti, and M. Chiani, "Cooperative Diversity in Wireless Sensor Networks", In Proceedings of WPMC'05, Aalborg, Denmark, pp. 1738–1742, 2005.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey", Computer networks, vol. 12, 2008.

[3] M. Srivastava, R. Muntz, and M. Potkonjak, "Smart Kindergarten: Sensor-based Wireless Networks for Smart Development Problem solving Environments", The seventh annual international conference on Mobile Computing and networking, July 2001.

[4] G. Hoblos, M. Staroswiecki, and A. Aitouche, "Optimal design of fault tolerant sensor networks", IEEE International Conference on Control Applications, Anchorage, AK, September, pp. 467–472, 2004.

[5] R.K. Patro, "Localization in Wireless Sensor Networks with mobile beacons", 23rd Convention of Electrical and Electronics Engineers in Israel, pp. 22-24, 2004.

[6] S. Gowrishankar, T. Basavaraju, D.H Manjaiah, and S. Kumar Sarkar, "Issues in Wireless Sensor Networks", Proceedings of the World Congress on Engineering, 2008.

[7] S. Misra et al., "Guide to Wireless Sensor Networks", Computer Communications and Networks, Springer-Verlag London Limited, 2009.

[8] S.K. Singh, M.P. Singh, and D.K. Singh, "Routing protocols in wireless sensor networks–A survey", International Journal of Computer Science & Engineering Survey (IJCSES), vol. 1, pp. 63-83, 2010.

[9] W.R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", Proceedings ACM MobiCom '99, Seattle, WA, pp. 174-185, Aug.1999.

[10] J. Kulik, W. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", Wireless Networks, vol. 8, no. 2, pp. 169-185, March-May 2002.

[11] Parvin, Shamsad, and S.R Muhammad, "Routing Protocols for Wireless Sensor Networks: A Comparative Study", Proceedings of the International Conference on Electronics, Computer and Communication, 2008.

[12] Heinzelman, W. Rabiner, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor network", System Sciences, Proceedings of the 33rd annual Hawaii international conference on System Sciences, IEEE, 2000.

[13] S. Lindsey, and C.S. Raghavendra, "PEGASIS: Power-efficient Gathering in Sensor InformationSystem", Proceedings IEEE Aerospace Conference, Big Sky, MT, vol. 3, pp. 1125-1130, March 2002.

[14] K. Naregal, and A. Gudnavar, "Improved cluster routing protocol for wireless sensor network through simplification", Advanced Computing and Communications (ADCOM), 2012 18th Annual International Conference on, IEEE, 2012.

[15] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks", IEEE communications surveys, vol. 7, no. 4, pp. 2–28, 2005.

[16] M. Weiser, "The Computer for the Twenty-First Century, Scientific American", pp. 94–101, September 1991.

[17] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", In Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 162-175, November 2004.

[18] R. Feng, S. Che, X. Wang, and N. Yu, "A credible cluster-head election algorithm based on fuzzy logic in wireless sensor networks", Journal of Computational Information Systems, pp. 1091–1103, 2013.

[19] G.V. Crosby, N. Pissinou, and J. Gadze, "A Framework for Trust-Based CH Election in Wireless Sensor Networks", Proceeding of 2nd IEEE Workshop Dependability and Security in Sensor Networks and Systems, IEEE Press, pp. 13–22, 2006.

[20] H.C. Leligou, P. Trakadas, and S. Maniatis, "Combining trust with location information for routing in wireless sensor networks", Wireless Communications and Mobile Computing, vol. l2, no.12, pp. 1091-1103, 2012.

[21] H. Deng, Y. Yang, G. Jin, R. Xu, and W. Shi, "Building a trust-aware dynamic routing solution for wireless sensor neworks", In Proc. IEEE GLOBECOM Workshop, pp. 153–157, December 2010.

[22] N. Poolsappasit, and S.K Madria, "A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network", 2011 International Conference on Parallel Processing (ICPP), pp. 138-147, September 2011.

[23] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures", Journal of Network and Computer Applications, Elsevier, vol. 35, no. 3, pp. 867-880, 2011.

[24] B. Finetti, "Theory of probability", J. Wiley and Sons, Inc., New York, vol. 2, 1974.

[25] Dhulipala, V.R. Sarma, N. Karthik, and R.M. Chandrasekaran, "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Network", Wireless Personal Communications, vol. 70, no. 1, pp. 189-205, 2013.

[26] G. Shafer, "A Mathematical Theory of Evidence", Princeton University Press, vol. 1, 1976.

[27] A. Jsang, and, R. Ismail, "The beta reputation system", In Proceedings of the 15th Bled Electronic Commerce Conference, pp. 41-55, June 2002.

[28] M. Momani, and S. Challa, "Survey of trust models in different network domains", International Journal of Ad Hoc, Sensor and Ubiquitous Computing, vol. 1, no. 3, pp. 1–19, September 2010.

[29] E.M. Daly, and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant MANETs", IEEE Transactions on Mobile Computing, vol. 8, no. 5, pp. 606-621, 2009.

[30] F. Bao, R. Chen, M. Chang, and J.H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169-183, 2012.

[31] G. Han, J. Jiang, L. Shu, J. Niu, and H.C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey", Journal of Computer and System Sciences, vol. 80, no. 3, pp. 602-617, 2014.

[32] F. Song, and B. Zhao, "Trust-based LEACH protocol for wireless sensor networks", In Future Generation Communication and Networking, 2008, FGCN'08, Second International Conference on, IEEE, vol. 1, pp. 202-207, December 2008.

[33] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, IEEE, pp. 1-10, January 2000.

[34] W. Weichao, D. Fei, and X. Qijian, " An improvement of LEACH routing protocol based on trust for wireless sensor networks", WiCom'09, 5th International Conference

on Wireless Communications, Networking and Mobile Computing, IEEE, pp. 1-4, September 2009.

[35] R.A Shaikh, H. Jameel, B.J. d'Auriol, H. Lee, S. Lee, and Y.J. Song, "Group-based Trust Management Scheme for Clustered Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 11, pp. 1698-1712, 2009.

[36] N. Wang, L. Gao, and C. Wu "A Light-Weighted Data Trust Model in WSN", International Journal of Grid and Distributed Computing, vol. 7, no. 2, 2014.

[37] R.A. Raje, and A.V. Sakhare, "Routing in Wireless Sensor Network Using Fuzzy Based Trust Model", 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), IEEE, pp. 529-532, April 2014.

[38] I. Sakthidevi, and E. Srievidhyajanani, "Secured fuzzy based routing framework for dynamic wireless sensor networks", 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), IEEE, 2013.

[39] X. Anita, M.A. Bhagyaveni, and J. Manickam, "Fuzzy-Based Trust Prediction Model for Routing in WSNs", The Scientific World Journal, 2014.

[40] T.K Kim, and H.S Seo, "A trust model using fuzzy logic in wireless sensor network", World academy of science, engineering and technology, vol. 42, no. 6, pp. 63-66, 2008.

[41] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs", IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, 2012.

[42] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks", In Wireless Sensor Networks, Springer Berlin Heidelberg, pp. 65-80, 2010.

[43] S. Rajaram, A.B. Karuppiah, and K.V. Kumar, "Secure Routing Path Using Trust Values for Wireless Sensor Networks", preprint arXiv: 1407.1972, 2014.

[44] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks", In Proceedings IEEE INFOCOM, pp. 1-9, March 2010.

[45] G. Theodorakopoulos, and J.S Baras, "On trust models and trust evaluation metrics for ad hoc networks", Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 318-328, 2006.

[46] R. Feng, S. Che, X. Wang, and N. Yu, "Trust Management Scheme Based on DS Evidence Theory for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2013.

[47] G. Wu, Z. Du, Y. Hu, T. Jung, U. Fiore, and K. Yim, "A dynamic trust model exploiting the time slice in WSNs", Soft Computing, vol. 18, no. 9, pp. 1829-1840, 2014.

[48] A. Tajeddine, A. Kayssi, A. Chehab, and H. Artail, "Fuzzy reputation-based trust model", Applied soft computing, vol. 11, no. 1, pp. 345-355, 2011.

[49] F. Cai, T. Fugui, C. Yongquan, L. Ming, and P. Bing, "Grey Theory Based Nodes Risk Assessment in P2P Networks", 2009 IEEE International Symposium on Parallel and Distributed Processing with Applications, IEEE, pp. 479-483, August 2009.

[50] J. Duan, D. Gao, C.H. Foh, and H. Zhang, "TC-BAC: a trust and centrality degree based access control model in wireless sensor networks", Ad Hoc Networks, vol. 11, no. 8, pp. 2675–2692, 2013.

[51] https://www.mathworks.in/products/matlab.

[52] K. Naregal, and A. Gudnavar, "Improved cluster routing protocol for wireless sensor network through simplification", 18th Annual International Conference on Advanced Computing and Communications (ADCOM), IEEE, 2012.

[53] D. Mahmood, N. Jayaid, S. Mahmood, S. Qureshi, A.M. Memon, and T. Zaman, "MODLEACH: A Variant of LEACH for WSN", 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE-2013), 2013.

[54] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, (2015) "An efficient distributed trust model for wireless sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1228-1237, 2015.

[55] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J.C.M. Teo, "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs", IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

LIST OF PUBLICATIONS

Published

A. Miglani, T. Bhatia, S. Goel, "Trust Based Energy Efficient Routing in LEACH for Wireless Sensor Networks", Proceedings of 2015 Global Conference on Communication Technologies, pp. 361-365, 2015.

Communicated

A. Miglani, T. Bhatia, S. Goel, "A survey of Trust Management in Wireless Sensor Networks", International Journal of Communication Networks and Information Security, vol. 7, no. 1, 2015.

A. Miglani, T. Bhatia, S. Goel, "An Energy Efficient and Trust Aware Framework for Secure Routing in LEACH for wireless sensor networks", International Journal of Sensor Networks, Inderscience Publishers, 2015.

VIDEO PRESENTATION

This is link to my YouTube video where I present brief summary of my thesis topic:

https://www.youtube.com/watch?v=UEfmz4hFpBc