# PSO based Trust management in Wireless Sensor Network

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

**Master of Technology**

in

**Information Security**


Submitted By

**Monia**

**Roll No. 801333012**

Under the supervision of:

**Dr. Sushma Jain**

**Assistant Professor**

**Ms. Sukhchandan Randhawa**

**Lecturer, CSE Department**



COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004


**June 2015**

## CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*PSO based trust management in wireless sensor network*", in partial fulfillment of the requirements for the award of degree of Master of Technology 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. Sushma Jain* and *Mr. Sukhchandan Randhawa* 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:

Monia

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

Dr.Sushma Jain
Assistant Professor,
CSE Department,Thapar University

Ms. Sukhchandan Randhawa
Lecturer,
CSE Department, Thapar University

**Countersigned by**

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

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

## ACKNOWLEDGEMENT

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life.

This work would not have been possible without the encouragement and able guidance of my supervisor's **Dr. Sushma Jain** and **Mr. Sukhchandan Randhawa**. I thank my supervisor's for their time, patience, discussions and valuable comments. Their enthusiasm and optimism made this experience both rewarding and enjoyable.

I am equally grateful to **Dr. Deepak Garg**, Associate Professor and Head, Computer Science & Engineering Department, a nice person, an excellent teacher and a well - credited researcher, who always encouraged me to keep going with work and always advised me with his invaluable suggestions.

I will be failing in my duty if I don't express my gratitude to **Dr. S S Bhatia**, Senior Professor and Dean of Academic Affairs, Thapar University, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct indirect help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my family whom I dearly miss and without whose blessings none of this would have been possible. To my parents, I owe thanks for their wonderful love and encouragement. I would also like to thank my brother, since he insisted that I should do so. I would also like to thank my close friends for their constant support.

Monia
801333012
ME(IS)

Date: July, 2015
Place: Thapar University, Patiala

# ABSTRACT

Wireless Sensor Networks (WSN) is widely distributed and powerful technology which is used in various fields but due to resource constraints, it is more vulnerable to attack. To mitigate from these attacks a technique is used called Trust Management. We propose a simple and an efficient algorithm which calculate the value of trusted node and find out the malicious node by using the optimized value of nodes. Due to homogeneous energy level of these sensor nodes; they generate the minimum spanning tree. In uniform and random distribution of sensor networks, nodes are categorized into different tiers like cluster head, cluster member and base stations. Some tiers follow hierarchical structure such as LEACH. A LEACH protocol is used in our proposed model PSO based Trust Management in Wireless Sensor Network where clustering is formed. Selection of cluster head is performed by using high energy and received signal, then it calculate the trust value on the basis of some parameters like packet forwarding factor, distance factor after calculation trust, it updates the trust value using PSO. To find out the best and optimized

value, a PSO approach is used which select the best weighted neighbor this approach enhance the working of the trust model. In this thesis, we analyze the consistency of clusters and the lifetime of the network. The simulation is implemented in MATLAB.

## Abbreviations

## Abbreviations used

| | |
|---|---|
| ACK | Acknowledgement |
| ADC | Analog-to-Digital Convertor |
| AL | Agent Launcher |
| ATRM | Agent based Trust-Reputation Model |
| BTM | Bayesian Theory of Model |
| DTM | Dynamic Trust Management |
| FTFSN | Flexible Trust Establishment Framework for Sensor Network |
| GBTMS | Group Based Trust Management System |
| GPS | Global Positioning System |

| | |
|---|---|
| GUI | Graphical User Interface |
| HOD | Human Opinion Dynamics |
| NFTMS | Novel Flexible Trust Management System |
| QoS | Quality of Service |
| RBTM | Reputation Based Trust Management |
| RFSN | Reputation based Framework for Sensor Network |
| TBSCR | Trust Based Secure Check Routing and Recovery Technique |
| TLSRP | Trust Dependent Link State Routing Protocol |
| WSN | Wireless Sensor Network |

**Table of Contents**

**List of Figures**

**Figure No. Figure Name Page No.**

**List of Tables**

**Table No.** **Table Name** **Page No.**

# Chapter 1

## INTRODUCTION

**1.1 Notion of Trust:** Trust plays a very important role in day to day life. This concept is defined as the reliability of believe. A trust is also define as the relationship between the one party which is called as *trustor* and other party *trustee* have right to hold their assets [4]. The person who acquires the property of another's benefit is called as *trustee* and the person who maintains the trust is called as *settlor*. It provides the trust between the parties which signifies approaches like managing and negotiation. As we know now-a-days accessing information over the internet is very important for everyone. People are totally relying on the internet services where unknown organization interacts and offer their services. So to provide the trusted information and which server is trusted on the basis of their certified statement it is necessary to build an trust management system [22]. Trust management is the backbone of trust model which is designed for special purpose and it maintain the relationship between customer and producer. Generally it consist three components:

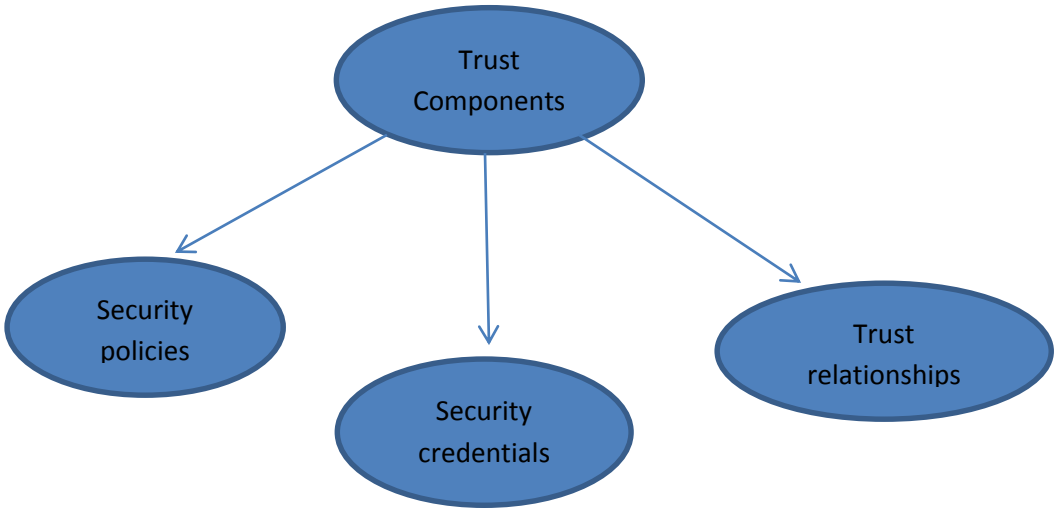


Figure: 1.1 Trust components

**Security policies:** The policies are made which is followed by two parties and also provide security between the two parties.

**Security credentials:** The signature must be verified before using the credential. Credentials are defined as a service which is used by both the parties. It would be duly signed by both, before it's used.

**Trust relationships:** It provides the framework about trust between the unknown parties, assign the keys and authorization.

Wireless Sensor Networks (WSN) is a mixture of little sensor node likewise called *mote* with every mote having an ability of detecting and sending the information to different nodes utilizing the radio recurrence. Every sensor monitor sends the gathered information to the sink node in the network. The sensor node sends processed data to the sink either by direct transmission or by utilizing the multi-hop transmission. Sensor nodes are distributed, deployed in a sensor field where it senses the relevant information and pass that information to the sink node the information which is passed by sensor nodes are route back to sink node and that sink node is connected to task manager (user) through internet or satellite. In multi-hop routing every sensor node sends the accumulated and interwined data by other sensor nodes to the base station. The range of these sensor nodes is very small, so that's why they cannot send data directly. It occurs an efficient solution in a wide variety of applications such as health care, homeland security, military, industry control, intelligent aircrafts and smart roads. Security plays an essential role in all of them and most advance in military surveillances. It can be described in a list of security requirements which include user authorization, node verification, data confidentiality, freshness, data integrity, secure localization and trusted resource allocation [1]. Sensor nodes are deployed in a hostile region where it is prone to attacks. WSNs are deployed in the physical world which makes it vulnerable and securely adheres in WSN. The more the dependency rate of data increases more the risk of transmission of secure data has also increased. Thus, providing security in WSN becomes very important. Due to restricted resources in WSNs, it is challenging to provide security functions like privacy, authentication etc. Hence, WSNs are more prone to malicious attacks like denial of service attack, routing attack, etc. However, to mitigate from these attacks and increase the reliability of information in WSN a trust based mechanism has been suggested [1]. WSNs have an unusual ability to mold the physical world, but with the growing technology profit of using WSN has led to some significant risk factors and misuse. So,

here question arise is that our information which is moving through tiny nodes are reliable data or unreliable? How can a user trust on that information? WSNs are prone to attacks so it is very important to provide security because of its resource limited.

### 1.1.1 WSN Applications

WSN application is categorized in two: Monitoring and Tracing (in fig 1.2). Monitoring is further categorized into health monitoring, military detection, environmental, business, public/industrial and habitat. Tracing is categorized into habitat, military, business, and public/industrial. Here are some few examples which are deploying in the real environment of WSN.

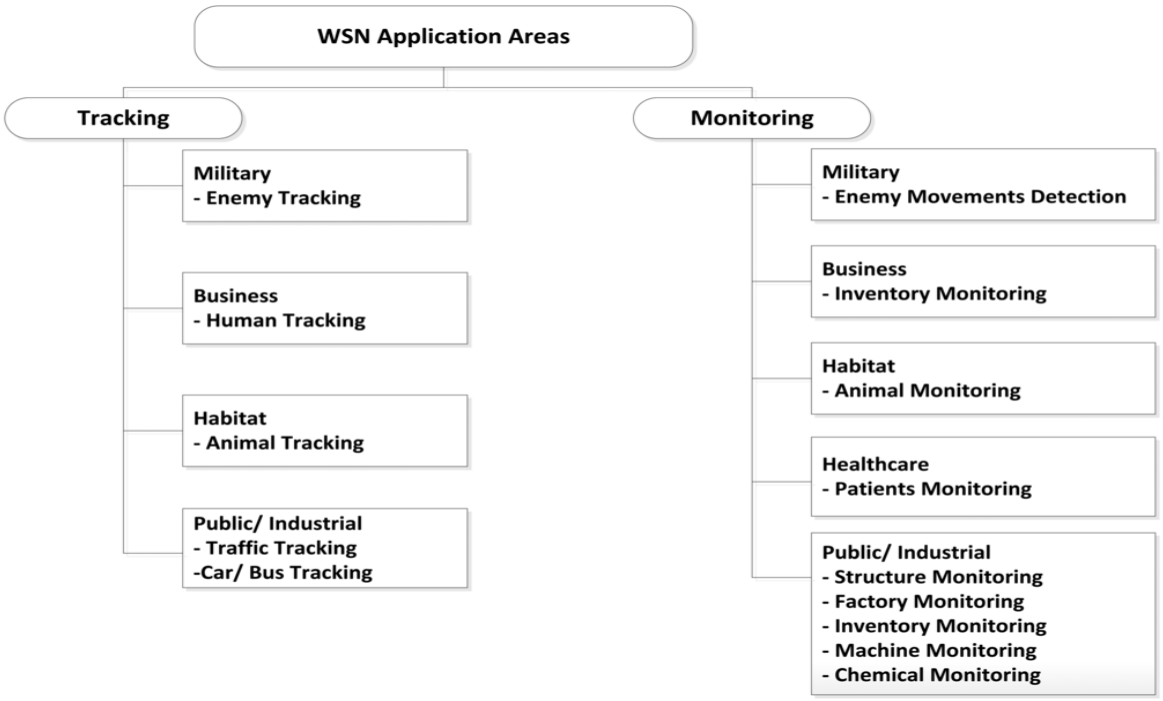


Figure: 1.2 Wireless Sensor Network applications

Pin ptr is a sensor device which has the capability to find out the location of shooter in the forest area. It detects and measure the time of arrival of the shoot and shock waves form shot [5].

Sensor nodes are set at different places in the tree so that it can monitor and stored the redwood trees in Sonoma, California. This is a case study called Macroscope of redwood

in WSN. Each sensor node measure the humidity, photo synthetic effect, radio waves, air temperature[6].

As per industry requirements the basic data needs to meet the application reliability. Semiconductor plants and oil tanker applications.

The underwater sensor node is used for monitoring the underwater species for a long time. These sensor nodes are used to monitor the underwater species like fisheries, temperature, climatic conditions, etc. These are the high speed optical communication using the point to point links. Sensor nodes are placed under the water to check the pressure, temperature and it contain cameras which record the habitat life under the sea.

MAX is a framework for human driven search of the physical world. It finds out the physical objects and to search out the people on the basis of their location. It works like a GPS(Global Positioning System) system to find out the landmarks rather than their coordinates. It uses the hierarchical approach which requires the objects to be tagged, substations as historic points and base station PCs to find objects. MAX is basically using crossbow motes [8].

CenWits is another sensor mote which is used for connection-less based tracking system. It is also called as the *research and the rescue system* [9]. These systems have very small number of memory and processing devices and also use a small amount of radio frequencies. Each sensor node use T-mote sky device, which consists of omni directional antennas, hardware interface board, microphone and a seismometer.

Volcanic monitoring is also one of the applications of WSN where sensor nodes collect relevant data and detect any event occur [10]. Each sensor node use T-mote sky device which consists Omni directional antennas, hardware interface board, microphone and a seismometer.

WSN also consist the health monitoring applications which enhance the wellbeing condition and patient checking like baby observing, cautioning the deaf, blood pressure controlling and firefighter vital sign monitoring. One of the best monitoring techniques is

baby glove which is used to monitor the baby's temperature, pulse rate and hydration. Baby glove consists small sensors where the baby is wrapped in between that glove.

ZebraNet is a mobile WSN which is used to track the animal migration. ZebraNet sensor nodes are deployed into the zebra's collar. It consist 16-bit TI microcontroller [11]. The purpose of this is to log each zebra position and find out their location using GPS readings and later use for analysis. It will give a great benefit to a biologist through whom they can easily watch their movements and positions during the day and night

.

**1.2 Necessity of Trust in WSN**

It can be depicted in a list of security necessities which include user authorization, node checking, information secrecy, data confidentiality, freshness and data integrity, secure localization and trusted resource allocation. As the dependency rate increased on the data, the more the risk of transmission of secure data has also increased. Thus, providing security in WSNs becomes very important. It is challenging to provide security functions like privacy, authentication etc. because of restricted resources. Hence, WSNs are more prone to malicious attacks such as denial of service attack, routing attack, etc. However, to mitigate from these attacks and increase the reliability of information in WSN a trust based mechanism has been suggested. Trust mechanism is a security mechanism to improve the reliability and to mitigate attacks. A new technique of getting security without using cryptography i.e. Trust based security in WSNs. Trust is "*The level of Reliability*" of another node to execute activities and can be framed by keeping a record of the activities with other nodes directly as well as indirectly. It figures the trust rate between the nodes. The conduct of the components of the network depends on trust model which can be very useful in a sensor network environment. It can not only help to take advantage of other security protocols, but also help the nodes to configure themselves against any change in the environment.[2]

### 1.3 Characteristics of trust and reputation in human societies

- Trust is very important in that environment where uncertainty and the participant must to depend on each other for their personal benefit.
- Trust is context sensitive. It is noticed that trust is a *three-part relationship* where A trust B to perform Z. The Z has some limits on trust relationship and Z has also some capabilities only in that particular subject which suit his context. The capability of B matter also which affect the level of trust A places in him.
- Trust is subjective. Some one's opinion on trust doesn't depend on the behavior of subject but also depend upon the behavior perceived by it.
- Trust is unidirectional. Based upon the knowledge in that particular subject is the agent's trust. The knowledge is observed by either owns observation or recommended by agent's friend[7].
- Trust cannot be transitive. For e.g if A meet B, he doesn't have trust on B but due to his friend F in which A trust and it sponsor B in that case either A have trust or it doesn't have trust. It totally depend upon the F's opinion of B which may be useful to A. Here witness is F which recommend B as a trust worthy person.

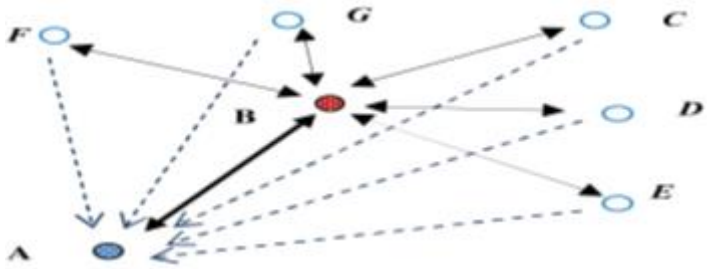


Figure:1.3 Direct and indirect recommendation

- Reputation is also one of the characteristics of trust. For e.g Customer has full faith on that organization those have good reputation in the market.
- Self-assurance belief. For e.g A patient trust a doctor to perform a specific task, asked to read and examine the X-ray result. A customer must trust the seller that they will provide the service that they advertise and will not disclose customer information.
- Willingness belief.

## 1.4 Classification of existing trust models

Trust and reputation can be assessed from two levels of reflection: *Individual Trust* and *System Level Trust*. In the first model trust is evaluated on the premise of direct interaction or information gave by others. This model is known as an individual trust model. Second model trust is evaluated on the basis of both trust and reputation model and protocol to interact with nodes. The second model is known as system model.

### 1.4.1 Individual level trust models

In the individual level trust model the interaction between the nodes are one to one where trust is calculated on the basis of successful interaction between the between the nodes. One way to gather information is like first-hand information about them which is calculated by the behavior of all the nodes. In this method each node requires to engage their interaction in a large number. In WSN's and MANET's both have distributed architecture of TRM (Trust and reputation Management) system because it is more feasible and provide the better extensibility. This model contains some components which included in individual level trust modeling. First-hand experience of node is that of past experience of that node assembled by other nodes. Whenever node received that data it becomes second hand information for that node only. After that node collaborates first hand and second hand information then they can map through predefined function and some aggregate function to evaluate the trustworthiness [3]. A decision is made by this evaluation. Then at the end interaction outcome evaluate. As explain in figure 1.3

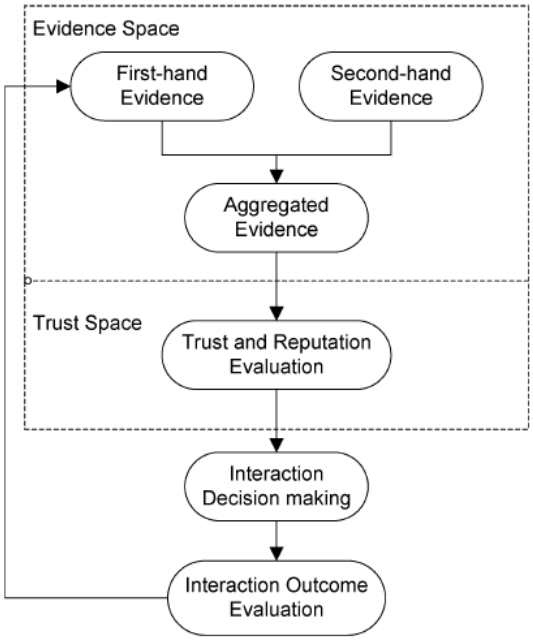


Figure: 1.4 Components of Individual level Trust Model

### 1.4.2 System-level Trust Model

The system level model consist a unique challenges. In wireless communication system, the degree of continuity can be measured by interaction of nodes between each other. In an efficient system-level trust model should have some measures like reward and penalty of nodes on the basis of their interaction which help to warn the malicious or selfish node[27]. Now-a-days most of the penalty measures are included in trust based models where those node are rewarded consider as good nodes and those are non-rewarding consider as bad nodes[28]. This attribute provides the unique challenge in system-level trust model. For a large number of networks where nodes are randomly changed their clusters can cause less number of interaction between them. So as a result nodes can dynamically join the cluster or leave the cluster. It propagates the trust evidence which is used for sharing the past experience of each node beyond the cluster. As explain in figure1.4

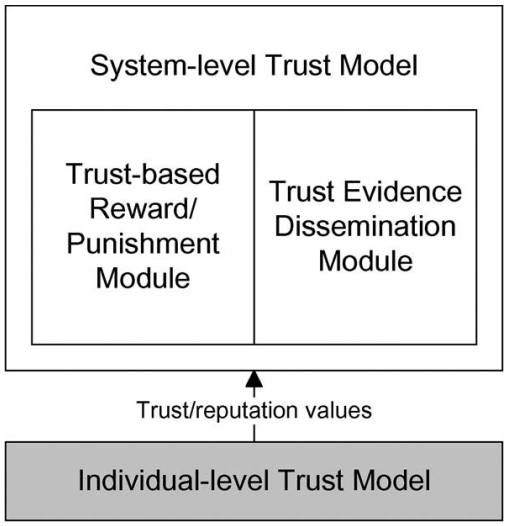


Figure: 1.5 Components in System-level Trust Model

### 1.5 Research challenges of Trust in Wireless Sensor Networks

Many researchers are working on these challenges, but none of them has fully integrated view of all these factors. These factors are very important because they are the algorithm and design protocols of WSN.

1. **Fault tolerance** is that technique where system has the ability to sustain the functionalities without any hardware or software error. So that, if any failure occurs system should have some backup or any procedure which doesn't consist any failure and take no loss. Some sensor node fails due to lack of power supply, due to environmental circumstance, physical damage and some malicious agents. Disappointment of one sensor node ought not to influence the entire sensor network errand. This is the reliability of adaptation of internal fault tolerance issue. Poission distribution of probability explains that failure doesn't occur in a time interval (0, t)

$$R_k(t) = e^{-\lambda k\, t,} \qquad (1)$$

   $R_k(t)$ is a fault tolerance and $\lambda_k$ is failure rate of sensor node and t is the time interim.
2. **Scalability** is defined as the number of sensor nodes can be increased on the basis of application. Depend upon application; it may increase from hundreds to thousands. So that our wireless sensor network should be scalable that it can adapt

the range from few sensor nodes to hundreds sensor nodes. We can calculate the density of the network by following formula

$$\mu(R) = (M \cdot \pi \Upsilon^2)/A \qquad (2)$$

Where M is number of scattered nodes in the area A and $\Upsilon$ is the radio transmission. $\mu(R)$ is the number of nodes within transmission radius of each node in the area.

3. **Production cost** as we know sensor network require a large number of sensor nodes and these sensor nodes are cost effective because each sensor node's cost define the cost of whole network. As sensor network is a large area which is cost effective and getting more expensive than deploying the whole sensor network. So that price of sensor node should be less.
4. **Hardware constraints** Sensor node consist four components i.e. sensing unit, a processing unit, a transceiver unit and a power unit. These component consist some additional features like localization finding, power generator and mobilizer. Sensing unit is made up of two sub unit sensors and Analog-to-Digital Convertors (ADC). The sensors send the analog signal to convertor it convert it into digital signal and send to the processing unit for process the data. Processing unit is used to manage the other component of sensor node it is the main component of sensor node. It is a small storage unit embedded on boards which manage procedure that enable sensor node to sense the data by running algorithms, protocols etc. Power units like solar cell. It is basically depend upon the application. Mobilizer is that which is used to move the sensor node for particular task. All of these subunits fixed in a small box. It should be small, compact and portable. These nodes should consume less energy, power, automotive, adapted to the environment.

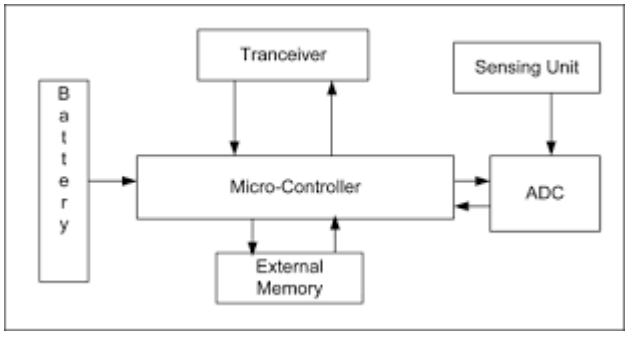


Figure: 1.6 Components of sensor node

5. **Sensor network topologies** hundreds of nodes are deployed in sensor network so a proper handling is require either to throw from the plan/missile or by human/robot. A careful handling is requiring to deploying the sensor nodes in the sensor field. Three phases of deployment

    a. **Pre deployment** Sensor nodes are deployed either by thrown or spot one by one in the sensor area.
    b. **Post deployment** after deployment, topology changes due to noise, jamming, availability, obstacles, position, mal functioning and task detail.
    c. **Redeployment of additional sensor nodes** sensor nodes can be added to the network as per requirement or if any failure occurs in any node so that redeploy at any time.

6. **Environment** sensor nodes are deployed in a hostile region where they mostly work unattended in far-flung geographic areas. They work in military field, to check the sea level and ocean environment, in the large machinery or in home/large building.
7. **Transmission media** sensor nodes are usually communicated through wireless media such as radio, infrared and optical media. Transmission must be available to operate this network. Infrared is license free so it would be easy to use infrared communication devices. These devices are easy to handle and cheap. Optical and infrared require line of sight between the source and the destination.

# Chapter 2

# RELATED WORK

## 2.1 State of the art research

In this chapter, we will discuss work done by researcher on Trust management scheme in wireless sensor network. Many researchers proposed different models to calculate trust values of sensor nodes and make them more efficient model in WSN. Some of them are as follows:

**RFSN:** Ganeriwal *et. al.* [13] have proposed a Reputation Based Framework For Sensor Network where trust value is calculated on the basis of reputation on the neighbor nodes . This layout is separate and label into two one is cooperative and other is non-cooperative. Reputation of trust value is calculated on the basis of the Bayesian trust formulation algorithm where it concludes that nodes have lots of interaction between each other so that reputation reach up to that point which is called as the stationary state (beta distribution). As the versatility rate of sensor node increase the publicized data get declines its execution. However, this trust model is essential for stationary systems so it can't adapt to vulnerability circumstances.

**ATRM:** Boukerch *et. al.[*14] have proposed an Agent based Trust and Reputation Management (ATRM) which is basically considered the power and bandwidth constraints. They just control the minimum overhead in time delay and extra message to manage the reputation and trust. The main working of this paper is to reduce the communication cost and latency by using the localization trust and reputation methodology. In ATRM it uses the mobile agents which are responsible for calculating the trust and it also reduces the bandwidth consumption. It requires that every sensor node consist the one mobile agent which is the manager who hold the trust values. ATRM is basically consist two aspects:

1) Initialization of network

2) Service provider

It constitutes some factors like the Agent Launcher (AL) which disseminates the mobile agents called Trust and Reputation Assessor (TRA) to each and every node. TRA comes under service provider aspect and provide the trust and reputation services. This aspect consist four sub service providers like r-certificate acquisition, t-instrument issuance, r-certificate issuance, and trust management routine [16].

- The r-certificate securing is pre transaction bennefit whose motive is to unveil the reputation value of the other node. This entire procedure can be performed by the exchange of the certificates (CerReq) certificate request and (CerRep) certificate reply messages. The node will be responsible for the service at the end whether it should begin a transaction or not.
- The t-instrument issuance is a post transaction service whose motive is to make sense of the trust value taking into account of the recent context. This whole process can be achieved by interchange of (InstrIssument) t-Instrument issuance and (ACK) acknowledgement message.
- The r-Certificate Issuance, executed same service and replica of TRAs based on the t-Instruments of their hosts. In the perspective of t-Instruments are context-precise, in this procedure single reputation value is computed in view of all contexts' value.
- The trust management routine is also likewise carried out by every replica TRA to keep up the evaluation table on its hosting node. In each round, the record which is older than specific threshold time will be wiped out from the evaluation table.

**DTM:** Guoewei *et.al*.[15] have proposed a Fuzzy-based Dynamic Trust Model (DTM) which uses fuzzy sets on the basis of grey theory to calculate the indirect and direct trust relationship. As we know that WSN consist limited resources, sometime nodes do not send the data to save their resources like bandwidth, energy and batteries. So to resist from these selfish nodes they propose a fuzzy based DTM. Only those with higher trust values can be chosen to forward packets and the nodes which are untrustworthy contain lower trust values which would be exempted from the trust metrics. Thus, their proposal also produces an incentive to force the selfish nodes to behave properly and again join the WSN. They also introduce the time slice scheme

which gives the maximum time to nodes to enjoy their service through this it will solve the problem of immediately interrupted link which decrease the trust value and it also increases the packet drop rate with number of selfish nodes and will increase the communication overhead. They conclude that their trust model is efficient and better performing in light weight where it detect the selfish node, pseudo selfish node, selection of recovery time..

**T-RGR:** Liu *et. al.[*16] have proposed a Resilient Geographic Routing (T-RGR) scheme which is very simple and easy trust management scheme. Their trust algorithm works when node forward packet to their closest destination on the basis of their localized information. This is basically used in ad-hoc networks and wireless sensor network but, it is defenseless against some diverse sorts of attacks so, it is necessary to mitigate from these attacks and provide the best solution. It uses the location information and determines the optimized decision. The basic idea is to have more and more trusted localizes sensor nodes. Sometime nodes still misbehave like dropping packets, etc. So in order to avoid this misbehave, they proposed a solution which uses the multi path routing and trust based route selection. In this scheme, each node monitors the behavior of its neighbor node. The value of the trust increases if neighboring node successfully forwards the packet, furthermore, in the event it drop the packet, then the source node will reduce its trust value by another steady parameter. If the trust value of a node is more prominent than the predefined threshold value, then the node will be pronounced as a trusted node, else it will be un-trusted node. This scheme is very easy and simple, but also uses fewer amounts of energy and memory. The main problem in their scheme is that they did not consider the security implications which make their scheme vulnerable against shared attacks.

**TLSRP:** Shaikh sahil *et.al.*[18] have proposed a new algorithm Trust Dependent Link State Routing Protocol which represents the trust worthy route between the source node to the sink node using trust (both direct and indirect) dependent on the link state routing protocol. Trust is calculated based upon some QoS parameters and also practices of other nodes. TLSRP is based on the geometric mean of the QoS parameter which permits the trusted node to participate in routing. This algorithm consist that it contains a number of

trusted routes and untrusted route from source node to sink node basis on different trust metric levels. The source node selects the best trusted route among many trusted route and select that route for communication and this trusted route is given by neighboring nodes trust level and route trust level. In the first part it concludes the trust path between the nodes and in the second part it concludes the trustworthy route from any node to sink node. The newly trustworthy route is used for communication between the source nodes to sink node which is free from malicious attacks.

**FTFSN:** Aivaloglou *et. al.*[17] have proposed Flexible Trust establishment Framework for Sensor Networks(FTFSN) where it consist both the properties of certificate-based and behavior-based trust management schemes. Some subset of nodes performs the certificate based scheme which evaluates the trust and some subsets of nodes perform the behavior based scheme these nodes are called as supervision nodes. The deployment of sensor node is performed by locally and distributed in the certificate validation scheme. The scheme is applicable only for static sensor networks where trust management signed the certificates when it is offline. Either node can be trusted or un-trusted nodes. Direct observation of trust node is calculated on the basis of some parameters and personal interaction experience of nodes within the radio range. Indirect observation is calculated on the basis of neighbor recommendation trust values. The trust level is calculated on the basis of their functionality and scope. Depending on routing protocols: many protocols have been published but to use it in trust routing mechanism is better and generic approach.

**TEM:** Huang *et. al.*[19] (2005), the authors proposed a Trust Evaluation Mode which is used to distinguish the trustworthiness of sensor nodes and to complete off the malicious nodes. They contemplate that several sensor node knows its own particular area with the synchronized time. In this model, the trust is calculated in a traditional approach. But, it can't update the trust. In Momani *et.al.*[20] (2005, 2006), a new trust scheme in WSNs was introduced. By using the traditional weighting approach, the authors merge direct and indirect information to calculate the trust.

**GBTMS**: Sheikh *et. al.*[21] has proposed a light weight algorithm for clustering where they preferred to calculate trust of a group of sensor nodes instead of single node. Two topologies were classified by GBTMS: (1) intragroup topology also known as distributed approach of trust management and (2) intergroup topology also known as centralized approach of trust management. For identifying malicious nodes, it provides some prevention mechanism.

On the basis of direct and indirect calculations, GBTMS calculate the trust values. Using direct observation, number of successful and unsuccesulf observation can be found between two nodes. Indirect observations recommend the trusted node about a specific node. All the cluster heads and sensor nodes were measured by the cluster head under which they lied.

This method is better from others on the parameter that it uses less memory as it uses unsigned integer trust, value and trust of group of nodes is calculated.

The main interest of this method is that it consumes less memory because it uses unsigned integer trust value and trust of a group of nodes is calculated. But more power and resources were required, therefore broadcast based strategies were used and on the basis of past experience, the trust is calculated in message delivery. A node can make a reputation and behave maliciously. But according to this paper good nodes are always honest.

**WTE:** Idris M. *et. al.[*22] have proposed Weighted-Trust Evaluation Scheme which is utilized to distinguish the compromised nodes checking its reported data. This approach obtained the less number of overhead. It adopts the hierarchical network architecture where it considers the flexibility and scalability. They have explained that their approach verified the detection of misbehaving nodes with less delay. The whole network may disrupt due to wrong information transmit through the compromised node or out of function node. So, detection of malicious nodes in the sensor network is a very important issue.

It consists two principles which is used for updating the weight of sensor nodes. In the first, at whatever point a sensor node is trade off and frequently sends its report uncertain with the final decision; its weight is liable to be diminished. At that particular time, sensor node considered a malicious node if its weight is lesser than the predefined

threshold. In the second principle, the weight decides to what degree a report may commit the final decision. It is worthy since if the report from a sensor node promote to be incorrect, it ought to be calculated less in the final decision. Despite the fact that weight value is refreshing dynamically, the chance of false likelihood is more [23].

**NFTMS:** Trakadas *et. al.*[24] have proposed a Novel And Flexible Trust Management System where the total transactions made by the node are defined by the trust ratio of the successful transaction. This model consists the trust management functionality which is shared over the whole sensor network. Whereas each node is in-charge of figuring out their personal trust value per relation in the network total direct and indirect data. The both direct and indirect trust values are used to calculate each node's trustworthiness.

$$T_m^{X,Y} = S_m^{X,Y} / ( S_m^{X,Y} + F_m^{X,Y} ) \quad (3)$$

Where S is successful transactions and F is unsuccessful transactions.

$$DT^{X,Y} = C^{X,Y} \times \sum_{m=1}^{k} ( Wm \times T^{X,Y}) \quad (4)$$

$W_m$ is the weight of each trust metric.

$$IT^{X,Y} = \sum_{j=1}^{n} (W_{X,N\,j} \times DT^{N\,j,\,Y}) \quad (5)$$

Where $W_{A,N\,j}$ is weight for recommended by jth neighbor.

$$T^{X,Y} = W_D \times DT^{X,Y} + W_I \times IT^{X,Y} \quad (6)$$

.

**TLEACH:** Fei song *et.al.*[12] have proposed Trust Based Low Energy Adaptive Clustering Hierarchy (TLEACH). It stores the working of the original protocol and provides the secure routing. Decision trust is basically the decision making in this scheme which evaluate the dynamics and separately for various decisions by situational trust. The trust management module is related with a trust based routing module which maintained

situational trust. In this scheme the direct trust and second hand information is calculated by a neighbor's situational trust with a novel trust model. This scheme increases the packet delivery ratio and detect more malicious node. They simplify the energy and communication overhead. By using the novel methodologies, trust management module is contracted for creating the trust relationships between the sensor nodes which provide efficient controlling, monitoring, interchange and evaluation of trust.

**RBTM:** Garth *et.al.*[32] have proposed an algorithm Reputation Based Trust Management which promotes the trusted cluster head by distributed keys. It introduces the concept of reputation based trust based management framework in wireless sensor network. With the help of trust based mechanism they prevent the cluster head from malicious attacks and also prevent from electing the compromised nodes. They use the probabilistic model which is used for electing and making the cluster head on the basis of trust. They use a beta distribution which is a simple and strong foundation on statistically. In this scheme they define the formation of clustering, as the clusters are formed, they find out the blacklisted and while listed nodes by maintaining their members. They assume that each node consist 3 keys one is master, pairwise and cluster key. Every node knows about the master key which is used for broadcasting. Each member share their cluster key with each cluster and group communication is in between their clusters themselves. Pairwise key is used for node to node communication.

**TBSCR:** Suparna Biswas *et.al.*[33] have proposed that a Trust Based Secure Check Pointing And Recovery Technique in MANET. They proposed a trust model with a combination of secure check pointing with the help of encryption techniques. If the mobile host is found to be trusted, then encryption technique does not require on check pointing because it is already secure. A number of clusters where each having a cluster head and cluster member. They communicate with each other through gateway nodes. A mobile host travels across the different cluster and leave behind their check point and logs in another cluster head. Check point node is also called as backup node where data is saved if any failure occurs, we can recover our data through this check point node. For collection the copy of checkpoint which is failing, a recovery node broadcast the message

to all cluster heads to forward the recovery of that node via gateway nodes. Recovery path is maintained, which is in between the recovery node and backup node and all the nodes in that route is called as reference node. It uses the concept of public key if any node finds out the entrusted node, then it may be encrypted the checkpoint and use fail mobile host's public key. Another side when the fail mobile host receives it decrypts the check point using private key. This scheme is summarized as:

1. A trust model is used to calculate the trust value of each mobile host.
2. After individual trust is calculated now next is to calculate the trust value of each of its cluster member. The trusted mobile host is found out by check pointing of mobile host so that it will retain the copy of check point.
3. Public cryptography is used for secure check printing.
4. A mobile host which is ready to save the checkpoint of a node can easily access that node.

**BTM:** Bayesian theory model is using by decades and proposed by (Sun *et al.*,2006) and applied thoroughly. This theory classified in two ways: one is objective and another is subjective. The objective is defined as that way where data are analyzed through statistical analysis and it does not consider the any subjective decision. Subjective way is that where it takes an argument of decision on the basis of confidence rate. In our best knowledge Bayesian theory is suitable to calculate the trust value.

Beta distribution system: is a series of trust and reputation model where it used beta modelling technique which calculate the trust value using positive and negative inputs. It uses the probability density function which evaluates the reputation score. It is denoted by beta(Þ/α/ß)

$$beta(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \qquad (7)$$

Where $0 \leq Þ \leq 1$, α, ß>0. With the limitation that the likelihood variable $Þ \neq 0$ if $\alpha < 1$ and $Þ \neq 1$ if ß< 1. The expected value of beta is $E(p) = \frac{\propto}{\propto+\beta}$ parameters like α and ß represent the ratings of r positive and s negative whereas ß = s+1 and α = r+1.

Beta distribution is combined with entropy model and Dampster-Shafer theory of evidence.

- Dampster-Shafer[25] analyze the trust network and Bayesian network uses the theory of evidence.
  b : Belief is define as that possible plan of action is true
  d : Disbelief is defined as that possible plan of action is false
  u : Uncertainty is defined as the measure of uncommitted conviction.
  a : Absence of evidence
  $\omega_x$ = (b, d, u, a) is denoted as subjective logic opinion.
  Where these components satisfy b,d,u €[0,1] and b+d+u = 1.

  Now, beta distribution with subjective logic, opinion become as:

$$E(p) = \frac{\alpha}{\alpha+\beta} \quad \text{where} \quad \begin{cases} \alpha = 2b/u + 2a \\ \beta = 2d/u + 2(1-a) \end{cases} \tag{8}$$

  Entropy Model: Entropy model is the concept of thermodynamics and information theory where it is used to measure the uncertainty of trust. Whereas Sun *et. al.*[26] has proposed a Bayesian based trust and entropy-based trust model.
  Entropy-based value is defined as

$$T = \begin{cases} 1 - H(p) & \text{for } 0.5 \leq p \leq 1 \\ H(p) - 1 & \text{for } 0 \leq p < 0.5 \end{cases} \tag{9}$$

  Where T is define as [Subject: action; agent] and p is define as [Subject: agent; action], $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ and H is the entropy function.
  This model assumes that more uncertainty less fluctuation of trust value.

**TPS-PSO:** Zhiwen, *et. al.* [30] have proposed a Trust Path-Searching Algorithm Based on PSO where it initialize the swarm particle and each particle balance their speed and searching space as per the information they have, after that they produce a new particle with a better result and optimize value. In the global search space they calculate the trust path in the network as the iteration moves one by one they get the best result and optimum solution in a short time period, it gives the better trust path. This algorithm utilizes PSO to inquiry the globally search non-second rate solution which is not the same as others. They proved the efficiency of their algorithm and also provide better performance than other algorithms. It can adjust the dynamic changes of an unpredictable network environment.

**LEACH-PSOv:** Jiang *et. al.* [31] have proposed a model which strengthens the LEACH-PSOv routing protocol of hierarchical architecture where they choose the node to transmit the data between the sink node to base station and they divide the network between the cluster, sub-cluster and cluster head of each cluster. This algorithm would extend the lifetime of the network. LEACH-PSOv extends the nearly 33% of time where no dead node. It also decreases the overlapping of secured range of each cluster where existing energy decreases the probability of lower energy. The cluster head node is elected on the basis of existing energy. This algorithm operates in a long time where it does not contain any dead node because of energy balance at each node. They have compared the LEACH and improved LEACH-PSOv where LEACH-PSOv proposed as per energy balance aspect of each node in the network. In LEACH first node died early, but in LEACH-PSOv node died after 300 rounds it means this algorithm consume less amount of energy.

# Chapter 3

# PROBLEM STATEMENT

In this specific chapter, the gaps which are exist in the present work. What is the problem proclamation, the objectives which are to be accomplished and system for accomplishing these goals are talking about.

## 3.1 Gap Analysis

In the literature review, we have discussed different model of trust management in WSN which are not as much as efficient. In the existing work talking about the loopholes exists:

1. In the existing approach, we have noticed that these existing models are only to calculate the trust value of nodes, but they did not explain how to recover the untrusted nodes.
2. Some existing model used the cryptographic techniques like public key, certificate, etc., but these techniques make the model heavier than before.
3. In the field of trust management most of the models evaluate the trust value on the basis of only one parameter, but trust can be calculated on the basis of more than one parameter.
4. In the existing model, they consume more energy and also have the problem of the long delay of transmitting messages.
5. Existing models evaluate the trust value, but they did not define the best and optimized route for transmitting the information from source to sink and sink to base station.

## 3.2 Problem Statement

Various models have been suggested in which some models define the trust calculation, management and routing where the problem is to design a simple and

an efficient trust management protocol. As we know that wireless sensor networks are scattered randomly, uniformly over the whole network. The location of the base station is fixed, but the corresponding nodes are uniformly distributed and mobile. So base station has unlimited power sources. The lifetime of the network is defined as the number of rounds completed till the particular node has sufficient energy, but in most of the models they only define the trust (direct and indirect) value on the basis of some parameter the disadvantage of that model is that they did not find out the malicious node. Some of the existing models do not have that capability to find out the best and optimized trusted route. In order to avoid this problem we have proposed a simple and an efficient rust management model which is a lighter weight trust model and can extend the lifetime of the network. After calculating the trust valued of sensor node our main objective is to find out the malicious or the dead node where we can roll back these nodes and by providing the technique of check pointing and recovery mechanism. At the end, our main purpose is to find out the best and the suitable optimized path which is used for routing and node updating. This thesis proposes both efficient and simple trust management and optimized routing in which is used to find out the best path and find out the malicious nodes in the sensor network.

### 3.3 Objectives:

1. To study the different techniques of trust models.
2. To propose a method of an energy efficient trust management algorithm.
3. To implement the techniques used in the proposed model
4. To test furthermore and also justify the output of the proposed technique utilizing diverse examination measurements.

# Chapter 4

# IMPLEMENTATION

In this chapter the trust model is used to evaluate the trust value of each and every node. We use MATLAB R2013a for implementation. MATLAB is utilized on the grounds that it gives a platform where processing is simple furthermore programming should be possible in an effective way. As we know that most of the work had already done in NS2, NS3 simulator in wireless sensor network, but using this technique, it gives the better comfortability and easily find out the bugs in the program. In our proposed trust model where we have calculated the trust value and after that using the parameter of distance and packet drop which is used to find out the malicious node and delay in the network. In the final output graph shows the number of dead nodes and alive nodes, number of cluster head selection on the basis of energy. It also reduces the consumption of more energy and light weight model where routing path is selected by using the approach PSO (Particle Swarm Optimization) which gives the best and the optimized path of trusted nodes.

## 4.1 Overview of MATLAB

MATLAB is a platform named as matrix laboratory which provide the numerical computing in multi-paradigm. It is also called as the $4^{th}$ generation language of programming. The researcher of Math Works Inc. Dr. Cleve Moler had composed the first form of MATLAB in 1970's. It is developed for the students so that they can access the LINPACK and EISPACK projects without any need of learning the FORTRAN language. By utilizing MATLAB, manipulation of matrix become easy, the information and functions can be plotted easily, calculations can be executed, an algorithm can be implemented, different client interfaces can be made furthermore interfacing should be possible with the projects which are actualized in diverse programming languages like JAVA, C++, C and Python. It is used for matrix theory, linear algebra and numerical

analysis. The MATLAB application is fabricated around the MATLAB scripting languages. It also supported, the object oriented programming which includes classes, inheritance, packages, pass-by-reference semantics. It support to develop the applications with GUI (graphical user interface). It likewise has firmly incorporated diagram plotting components. Many technical and computing problems can solve by using MATLAB. Many researchers used MATLAB for their simulation. MATLAB is also very useful in the field of Sensor network where it consists inbuilt sensor signal, routing Simulink and various tool boxes like signal processing toolbox, sensor network etc.

### 4.2. Network Model

The network model for proposed algorithm is formed by deploying 100 sensor nodes randomly and uniformly in the network area $100 \times 100m^2$. Initially, each sensor node has the same amount of energy 0.5j. This energy is consumed by transmission of data from the source to the base station. Every node has the capability to sense the data and send to the sink node and further. So to simplify the network model and overcome from delay we use the hierarchical structure called LEACH.

#### 4.2.1. Hierarchical method

In this sort of routing system where nodes assume to be in different role play for transmitting and accepting information. A percentage of the node is in charge of processing the data and other nodes for communication. Some nodes can be utilized for detecting the objective territory. Hierarchical routing is very much popular in sensor network where it consist two layer architecture one is for selection of cluster head and another tier is for routing information. After selection of cluster head, its responsibility to collect the aggregate data and transmit that data to the base station. Formation of clustering and assign a task to the cluster head leads to an energy efficient and scalable network.

**4.2.1.1 LEACH (Low Energy Adaptive Clustering Hierarchy)** have proposed by Wendi B. Heinzelman where it describes the cluster based routing that uses the randomly nodes and supply the energy load evenly to theses sensor node in the network. The procedure is ordered into two phases, one is set-up phase followed by steady phase. The

backbone of this protocol is to build a cluster and communication between them. In first set-up phase, election of cluster head is based on when each node sends the broadcast message to the rest of nodes and then non-cluster head concludes that whether they join the received signal or not. In second steady-phase, non-cluster head nodes transmit data to their corresponding cluster head where aggregate data is transferred from cluster head to base station with one hop. This is the first round in the next round again this whole procedure followed where it distributes the energy among all nodes.

A predefined value of T ( n ) where random number is assign to every node between the 0 and 1. If a umber is less than the predefined value then node would be selected for cluster head. At the point when only a node of not being chosen as cluster node has left out, then T(n) of the node would be 1. i.e. node become cluster head.

$$T(n) = \begin{cases} \frac{P}{1-P(rmod(1/P))} & if(n \in G) \\ 0 & otherwise \end{cases} \qquad (10)$$

Whereas p is the probability of selection of cluster head in the whole cluster. r is the maximum rounds. G is the node which has never become head node. After the election of cluster head node, it will transfer the information to other nodes and nodes join their clusters dynamically base on some factors.

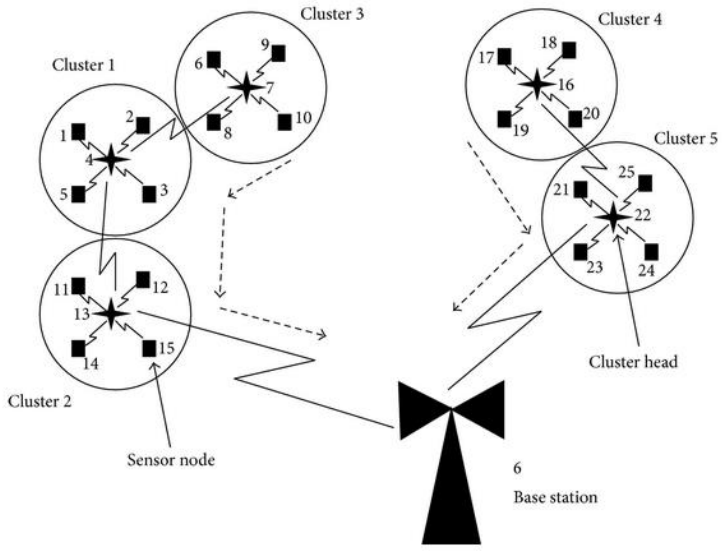


Figure 4.1: Two level Hierarchical structure

### 4.3 System Model

The system model is categorized into different components which deal with energy consumption, environment, sensor nodes, base station.

- Base Station: It is a powerful sensing unit which is also called as central processing unit of sensor network. It gathers all the information from the sink node and also from the sensor nodes.
- Sensor Node: Each sensor node has ability to sense any event and transmit data to other sensor nodes.
- WSN: it is a network area where numbers of sensor nodes are deployed by uniformly and randomly.
- Energy: Initial energy of node is $E_0$. As the number of rounds increases the energy of node become also reduce. The nodes which have sufficient energy can transmit data while those haven't they can remove from the network.

#### 4.3.1 Trust model

Trust based management model provides the trust on the behavior of different nodes over the network. Trust mechanism is a security mechanism to improve the reliability and to mitigate attacks. A new technique which provides security without using cryptography i.e. Trust based security in WSNs. Trust is defined as "The degree of Reliability" of another node to perform some actions which can maintain the record of the action with other nodes directly as well as indirectly. It calculates the trust rate between the nodes. The behavior of the elements in the network depends upon the trust model which is very useful in a sensor network environment. It cannot help to take advantage of other security protocols, but also helps the nodes to configure themselves against any change in the environment [29].

In WSN, every node forwards the packet to another node by hoping technique according to the routing protocol. Trust has calculated either by their own observation of individual nodes or recommendation of other nodes for their past experience. This trust value is used to find out the secure path between the source to the destination. Neighbors who have highest trust value is used to send the packets and who have less than the

defined value of trust is considered as a malicious node. Our scheme is divided into some categories where it consists: trust observation, trust calculation, trust ranking, trust recovery.

- Trust observation is calculated in every node either by direct relationship or indirect relationship between the nodes. It is calculated on the basis of any metric value.
- Trust Calculation is evaluated by using our proposed an efficient trust algorithm which evaluates the trust value of every node.
- Trust ranking is given on the basis of trust values and metrics where trust is in order listing.
- Trust recovery is the process to recover the malicious node and those nodes who have lost their data due to some conditions like environmental, attacker, signal interference etc. Check pointing and recovery technique is used to recover the lost data.

Our model consist some assumptions:

1. All links in between the nodes are bi-directional and all nodes have same transmission range.
2. A packet send by one node is received by other nodes who are in their transmission range.
3. Some malicious node also exists which can use more resources or bypass the traffic.
4. Signal fluctuation and collision may cause the packet drop.

#### 4.3.1.1 Trust metrics

Metrics are used to determine the information on how many packets forward and how many drops. By using some probability of successful interaction between the nodes a direct trust and indirect trust is evaluated.

$$S_{i,j}^{d}(t) = \frac{F}{R}_{i,j}(t) \qquad (11)$$

Where Fi,j (t) denotes the no. of packet forwarded correctly by node j at time t, Ri,j (t) denotes the no. of packets successfully received by node j from node i at time t. $S_{i,j}^{d}$ (t) direct trust calculated.

$$S_{i\,j}^{m}(t) = \frac{1}{n}\sum_{k=1}^{n} \quad S^{d}_{i\,j}(t) \qquad (12)$$

$S_{i\,j}^{m}$ (t) is indirect trust value.

So finally a metric is obtained where direct trust and indirect trust value is stored.

#### 4.3.1.2 Trust relationship

In this category, a node collects the direct and indirect trust values in various distinct trust metrics. $S_{i,j}^{d}$ (t) is the direct hand observation which determines the trust value on the basis of packet forwarding and receiving. On the other hand, indirect trust value is calculated $S_{i\,j}^{m}$ (t)

$\frac{1}{n}\sum_{k=1}^{n}$ $S^{d}_{i\,j}$ (t) by the recommendation of other nodes to their past experiences.

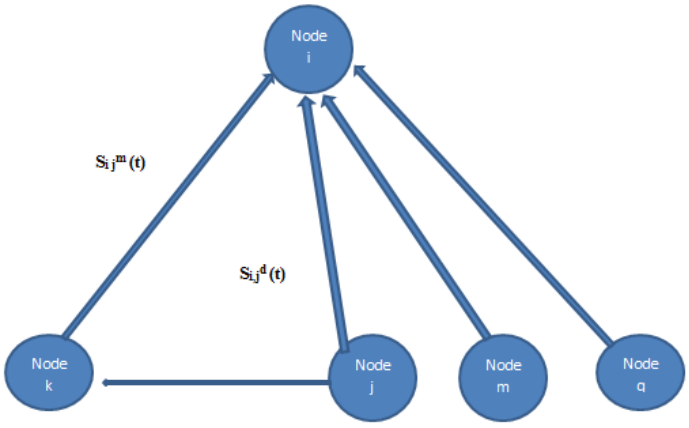


Figure: 4.2 Trust Relationship between node i, j and k.

For example node i have direct interaction with node j, while node j has direct interaction with node k. Then node j may forward the direct trust value of node k to node i. So that node i can use the indirect information to calculate the trust level of node k.

On the basis of this we can calculate the trust level of nodes by using the probability of successful interactions where we can define fully trust node, relatively trust node, general trust and un-trusted respectively

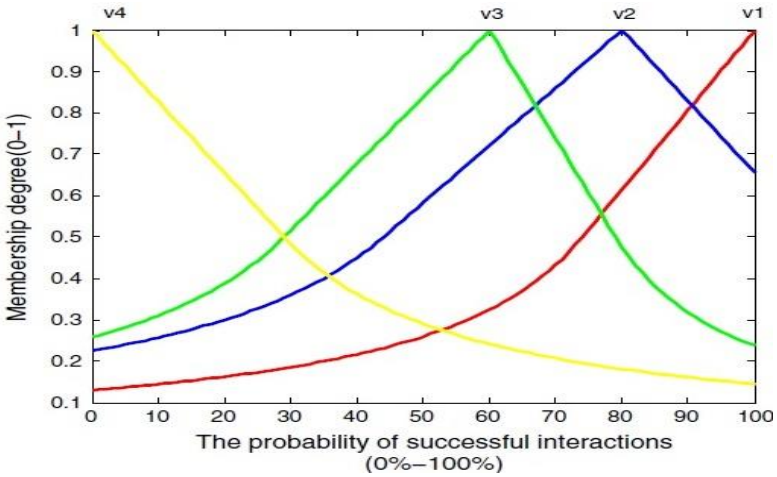


Figure:4.3 Trust degree of each metric

The x-axis represent metrics value and y-axis represent the membership degree whereas v1, v2, v3, v4 are degree of membership.

In our proposed model each and every node calculates the trust value of its neighbor based on their recommendation and direct interaction.

**4.3.2 Particle Swarm Optimization (PSO)** is an optimization algorithm which is used to solve the iteratively problem to find out the best and good quality of solution. It optimizes and enhances the issues of indicated by a progression of candidate solutions. It is the process, where each bird flew according to their better region based on the fitness function It searches the large number of spaces where every candidate has their own assumption. It searches as a group of multi-objective from source node to the target node. Every bird can fly with a certain velocity in D-dimensional seeking space. Let the seeking space is D-dimensional and the location of the i particle is explained as $x_i = (x_{i1}, x_{i2},\ldots\ldots, x_{id})$, its velocity is $v_i = (v_{i1}, v_{i2}, \ldots\ldots, v_{id})$ ,till at that point, the best area that the ith particle has looked is $p_i = ( p_{i1}, p_{i2},\ldots\ldots\ldots, p_{id})$ till at that point where they et the best location for all articles i.e. $p_g = (p_{g1}, p_{g2,\ldots\ldots\ldots}, p_{gd})$. The parameters of D-dimension $(1\leq d\leq D)$. The basic formula of PSO algorithm is shown as

$$V_{id}(t+1) = w \times V_{id}(t) + c_1 \Upsilon_1 \times (p_{id}(t) - x_{id}(t)) + c_2 \Upsilon_2 \times ( p_{gd}(t) - x_{id}(t)) \quad (13)$$

$$V_{id} = V_{max}, \text{ if } V_{id} > V_{max} \quad (14)$$

$$V_{id} = V_{max}, \text{ if } V_{id} < V_{max} \quad (15)$$

$$x_{id}(t+1) = x_{id}(t) + V_{id}(t+1) \quad (16)$$

Where $r_1$ and $r_2$ re random numbers between 0 and 1; c1 and c2 are coefficient of acceleration, w is the inertia, $v_{max}$ is the constant. The speed of the birds(particle) cannot exceed by maximum speed set.

Whereas ω(t) is the inertia weight which is used to adjust and maintain the global and local search.

$$\omega(t) = 0.9 - \frac{t}{Max\ Number} \times 0.5 \quad (17)$$

While, Max Number is the number of maximum iterations.

**Steps of PSO**

1. First step is to initialize the particle population by allotting areas (X-vector) and velocities (V-vector) always start from zero.
2. The fitness of individual particles is calculated and records the best fitness $P_{best.}$
3. The highest fitness $G_{best}$ is calculated by individual and their postion is store.
4. Update and modify the particle position $P_{best}$.
5. End if the condition is met.
6. Otherwise Go to step 2.

**4.3.2.1 Types of PSO**

1. **$G_{best}$ PSO**

   It is defined as the best value, followed by the particle swarm analyzer is the best value got so far by any particle in the population. It depicts that as the best value followed by PSO is the best value acquired by any particle in the area of that particle[34].

2. **$P_{best}$ PSO**

It is defined as the best solution (fitness) it has accomplished so far where each particle finds out the best solution in its solution space by keeping the track of all its coordinates [34].

Table: 4.1 Summarize the variables in PSO

| | |
|---|---|
| v | Particle velocity |
| x | Particle position |
| t | Time |
| c1, c2 | Learning Factors |
| ϒ1, ϒ2 | Random number [0,1] |
| $P_{id}$ | Particle's best position |
| $P_{gd}$ | Global best position |
| ω | Inertia weight |

**4.3.2.2: Pseudo Code of PSO[37]**

Algorithm 1 Initialize

```
for each particle i in S do
  for each dimension d in D do
    x_{i,d} = R(x_min, x_max)
    v_{i,d} = R(-v_max/3, v_max/3)
  end for loop
  pb_i = x_i
  if f(pb_i) < f(gb) then
      gb = pb_i
  end if
end for
```

Algorithm 2 Particle Swarm Optimization

1: Initialize
2: Repeat
3: for each particle i in S do
4: if $f(x_i) < f(pb_i)$ then
5: $pb_i = x_i$
6: end if
7: if $f(pb_i) < f(gb)$ then
8: $gb = pb_i$
9: end if
10: end for
11: for each particle i in S do
12: for each dimension d in D do
13: $V_{id}(t+1) = w \times V_{id}(t) + c_1 \Upsilon_1 \times (p_{id}(t) - x_{id}(t)) + c_2 \Upsilon_2 \times (p_{gd}(t) - x_{id}(t))$

$x_{id}(t+1) = x_{id}(t) + V_{id}(t+1)$

14: end for
15: end for
16: it = it +1
17: until it > MAX_ITERATIONS

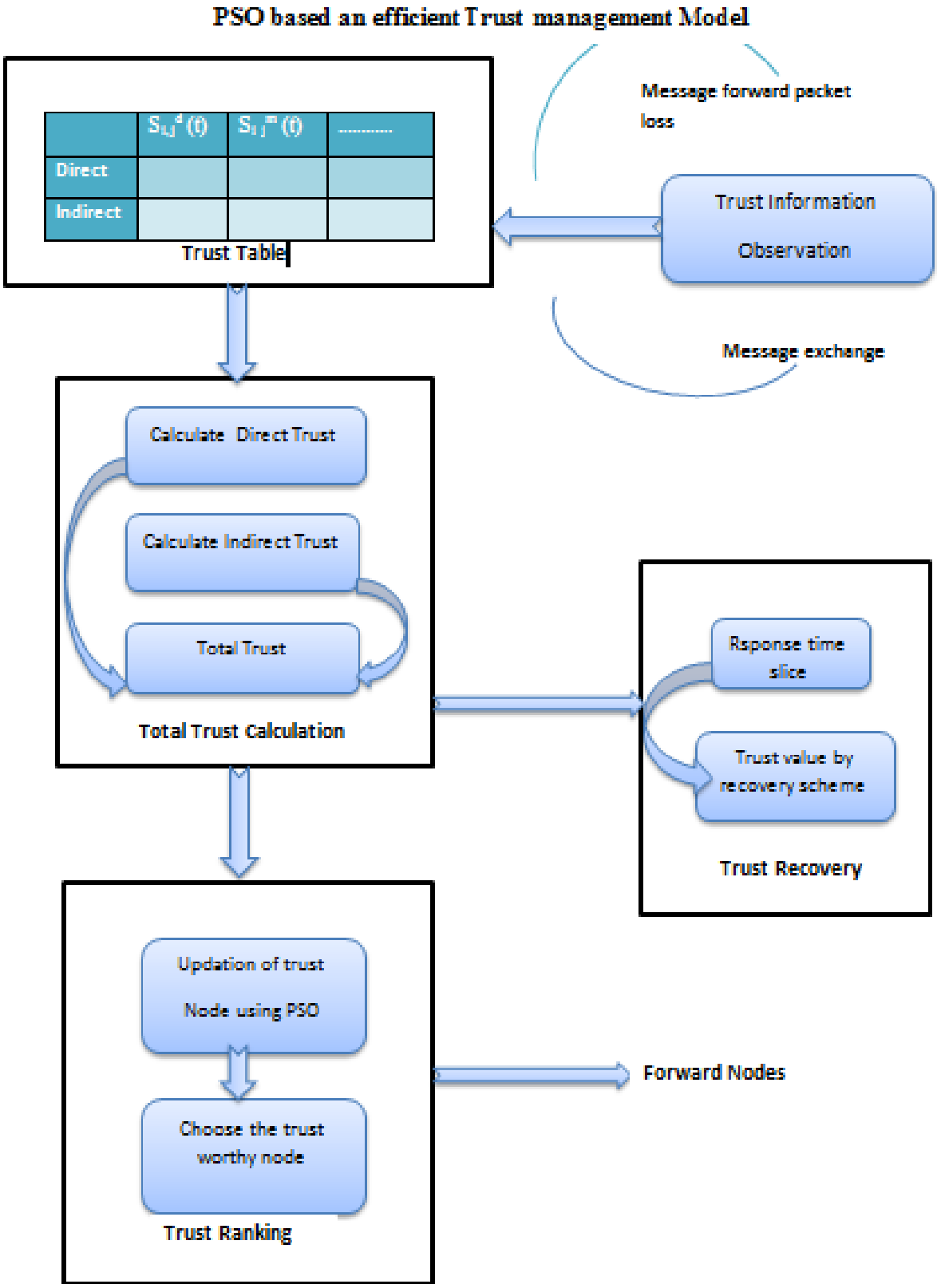


Figure: 4.4 Proposed PSO based Trust model

### 4.3.3 An improved and efficient PSO based Trust algorithm

Algorithm: PSO based Trust management of the node

**Step 1:** Selection of cluster head only those nodes who have larger energy than threshold energy is consider as cluster head.

$$E_{th}=E_0*[1-\theta\ (n-r)] \quad (18)$$

$E_{th}$ – threshold energy E0 – initial energy Ø – energy attenuation factor which lies in between 0 and 1.

**Step 2:** Initialization of cluster head and adjusting its position initialize the cluster head Ch= 0 and determine its closest neighbor on the basis of received signal strength.

$$D = Ø* \sqrt{1 \div \pi K} * M \quad (19)$$

Where D is the distance, K is the number of cluster head, M is the side length of square area, Ø is the adjusting factor.

Number of cluster head near to the node can be calculated as

$$M^{ch} = W_1 ( E_{left} \div E_0 ) + W_2 ( S_{i\,j}(t) \div \sum S_{i\,j}(t) ) + C_{ch} \quad (20)$$

$W_1, W_2 \in [0,1]$ are weight factors, $E_0$ initial energy, $E_{left}$ remaining energy, $\sum S_{i\,j}(t)$ sum of trust nodes. $C_{ch}$ cluster head count.

**Step 3:** Calculate the individual trust value of node

$$S_{i,j}{}^{d}(t) = \frac{F}{R}_{i,j}(t) \quad (21)$$

Where Fi,j (t) denotes the no. of packet forwarded correctly by node j at time t, Ri,j (t) denotes the no. of packets successfully received by node j from node i at time t. $S_{i,j}{}^{d}$ (t) direct trust calculated.

$$S_{i\,j}{}^{m}(t) = \frac{1}{n}\sum_{k=1}^{n} \quad S^{d}{}_{i\,j}(t) \quad (22)$$

$S_{i\,j}{}^{m}$ (t) is indirect trust value.

**Step 4:** Calculate the total trust value

$$S_{ij}(t) = w_1 S^{d}_{ij}(t) + w_2 S^{m}_{ij}(t). \quad (23)$$

Calculate the trust rate, let's take a node $S_{ij}(t)$ denote the degree of trust in its neighbor j of node i at time t. The trust range lies between 0 to 1.0 denotes the distrust and 1 denotes the ideal trust. $S_{ij}(t)$ is the total weighted average of two.

**Step 5:** Updating the node using the PSO approach where the velocity and position of particle updated

$$V_{id}(t+1) = w \times V_{id}(t) + c_1 \Upsilon_1 \times (p_{id}(t) - x_{id}(t)) + c_2 \Upsilon_2 \times (p_{gd}(t) - x_{id}(t)) \quad (24)$$

$$x_{id}(t+1) = x_{id}(t) + V_{id}(t+1) \quad (25)$$

Where $\Upsilon_1$ and $\Upsilon_2$ are random variables between 0,1; $c_1$ and $c_2$ are coefficients of acceleration.

# Chapter 5

## SIMULATION RESULTS

In this section we use simulation to study the performance of our system model to calculate the optimal value of the trusted values of each node in an efficient manner. The experimental result shows the working of trust model and find out the optimized value by using the PSO approach. In this section we have concluded the optimized result of trusted sensor nodes, evaluate the trust value of each and every node, find out the best weighted neighbor nodes, throughput of nodes, the number of dead nodes, number of alive nodes, number of packet loss to base station, count of cluster head per rounds.

**Table 5.1 Simulation Parameters**

| Simulation tool | MATLAB R2013 |
|---|---|
| Dimension | 100 × 100 |
| Simulation time | 30 seconds |
| Reliability | Packet loss, energy consumption |
| Mobility | Energy consumption, |
| Number of nodes | 100 |
| Initial energy | 5J |
| Initial trust value | 0.5 |

The figure 5.1 depicts the dimension (100*100) x-axis and y-axis where nodes are uniformly dispersed within the area.

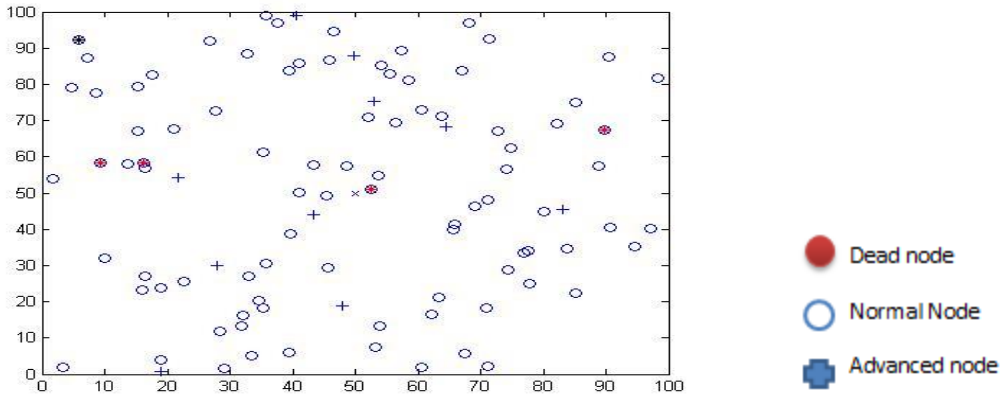


Figure 5.1: Randomly nodes distribution

There are two types of nodes advance nodes and normal nodes. Advance nodes are those nodes which owns a more energy than the normal nodes Eo is the initial energy and $E_o(1+a)$ consist the initial energy of advance nodes. Dynamically cluster head selected where $a_{max}$ is the maximal energy. Initally node $s_i$ assembled with initial energy $E_o(1+a)$ i.e it is $a_i$ times more energy than the lower bound $E_o$. The figure 5.2 depicts the formation of cluster head in the whole sensor area, where energy is transmitted between the nodes and they select the higher energy node as the cluster head. These cluster head are also selected by their neighbor nodes in that particular area. As every count, the number of cluster head changes as per number of iterations.

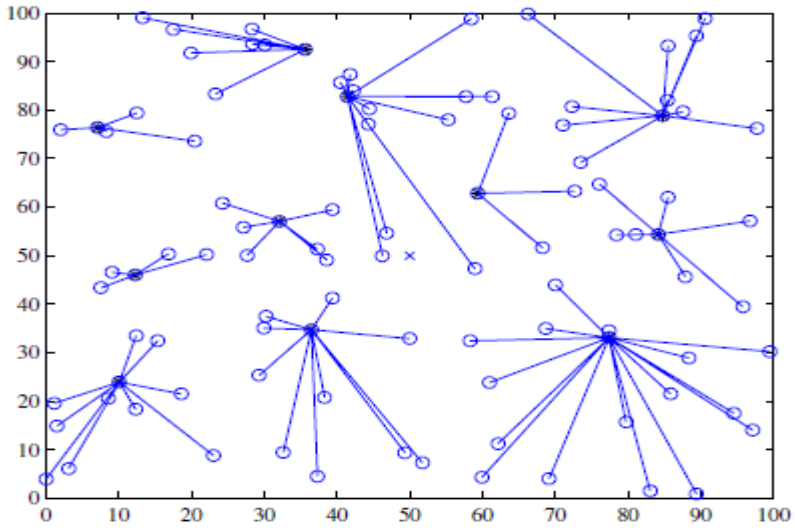

Figure 5.2: Cluster head selection

Cluster head is elected on the basis of the probability ratio between the residual energy of each node and the average node energy in the network.

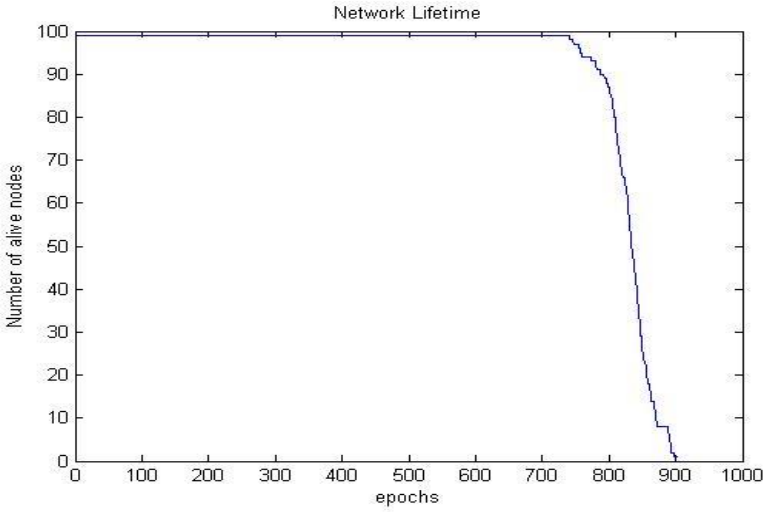


Figure 5.3: Network Lifetime

In figure 5.3 x-axis represents epochs and y-axis represent the number of alive nodes. In an homogeneous network all nodes have same initial energy. In LEACH protocol every node become cluster head exactly after every $\frac{1}{popt}$ rounds. Epochs are $\frac{1}{popt}$ number of rounds in the sensor network.

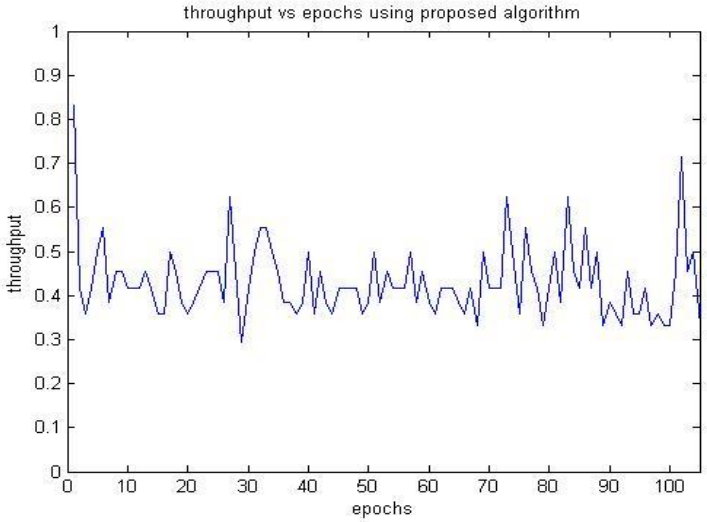


Figure 5.4: Calculate the throughput using the proposed algorithm

In figure 5.4 where x-axis represent the throughput and y-axis represent the epochs. It calculates the throughput of the network in a particular time period. It is define as the rate of successful transmission of packets delivery over a channel in epochs using proposed algorithm.

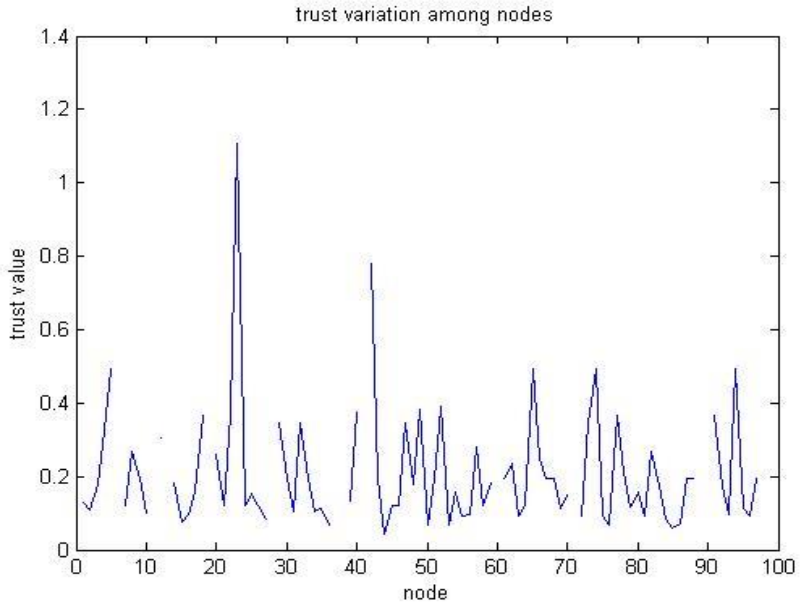


Figure 5.5: Trust variation of sensor nodes

This figure 5.5 represents the trust value of each node where x-axis defines as sensor nodes and y-axis defined as the trust value of sensor nodes. The variation represents the trust value varies from node 1 to node 100.

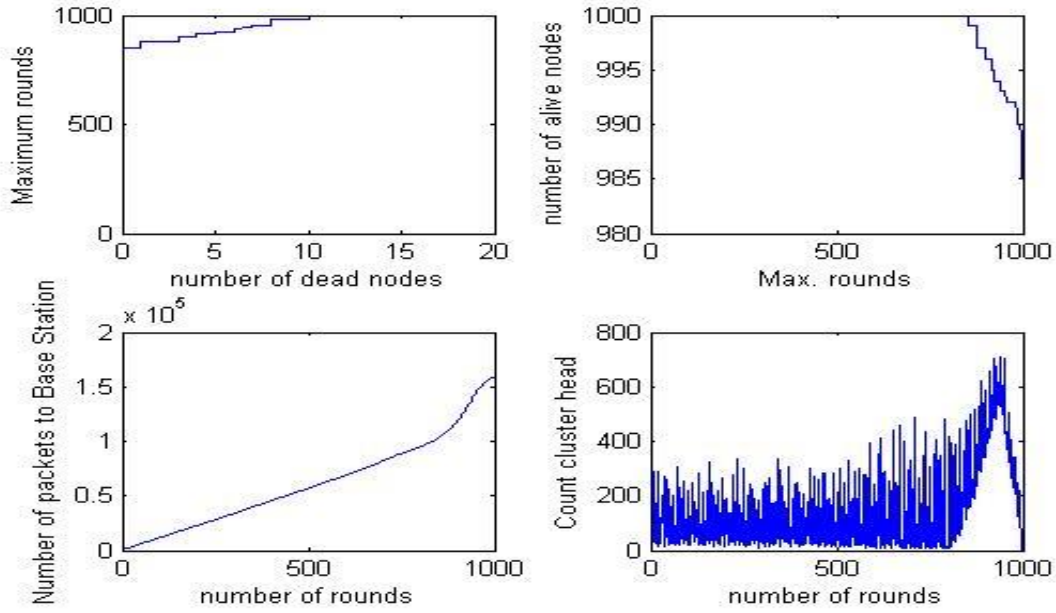


Figure 5.6: (a) Plot represents the number of dead nodes (b) Number of alive nodes (c) Plot represent the number of packets received at Base station per round. (d) Count of cluster-head.

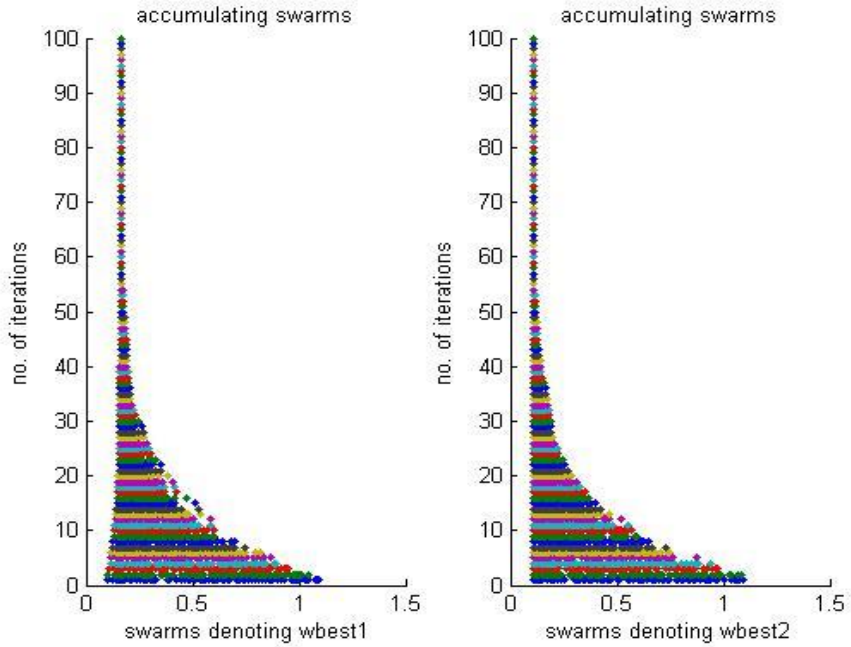


Figure 5.7: Optimized value using PSO (Particle Swarm Optimization)

The figure 5.7 depicts that x-axis denote the swarm wbest1 and wbest2 while the y-axis denotes the number of iterations. Iterate in accordance with formula until it reaches the maximum number of iterations. PSO chooses the best optimize value out of the solution space where it accumulates the swarm particles those are randomly distributed.Wbest1 and wbest2 are weights which we use to calculate the best weight neighbor and cluster head adjustment. As the number of iterations increases the optimized value of weight also decreases.

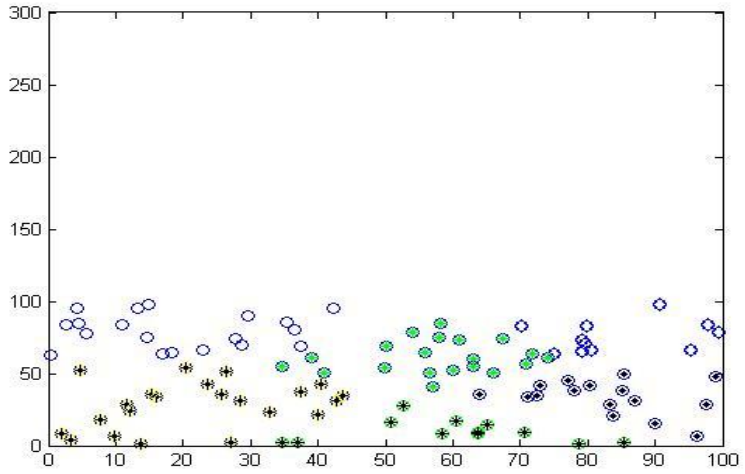


Figure 5.8: Best weighted neighbor and cluster head adjustment

The figure 5.8 depicts that green dots are the best weighted and also most trusted neighbor cluster nodes which is used to send the confidential information in the whole network whereas, black nodes are dead nodes. The range of nodes considers as 100 and initial energy of sensor nodes is 0.5nj/node this energy is used to transmit the packet to the base station but now its energy get increases. Figure 5.8 shows the best weighted nodes which can be used to find out the best suitable path for data packets.

## Conclusion and Future scope

In this work, a technique, namely PSO based an efficient Trust based management model have proposed. The simulation results show that the algorithm perform the result near to optimal. From this we conclude, the trust value of each node, network lifetime, throughput of network, number of alive nodes, dead nodes, and packet delivery to the base station. This algorithm selects the non-inferior solution and find out the best optimized solution. It can adjust to the dynamic changes of a complex network. To some extent this approach is simple and efficient in terms of memory and also effective in fraudulent case. Our proposed model concludes that they are sustaining at the node in finding the trust on any neighbor node and to evade some suspicious nodes. This approach can increase the network lifetime. As a future reference it can be thought as a network using the optimal trusted path.

In future, this network can be more reliable by calculating the trusted path between the source node to the destination node. The idea of accomplishing some level of fulfillment in the security arrangement could be extended beyond the wireless sensor network. However, some efforts are required to tune various models like HOD (Human opinion dynamics) where it gives rise to the development of various kinds of opinion in a society. This technique can be used to solve the optimization problems.

## REFRENCES


[1]. Zahariadis, Theodore, et al. "Trust management in wireless sensor networks." European Transactions on Telecommunications 21.4 (2010): 386-395.

[2]. Gago, M., Rodrigo Roman, and Javier Lopez. "A survey on the applicability of trust management systems for wireless sensor networks." Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on. IEEE, 2007.

[3]. Ramchurn, Sarvapali D., Dong Huynh, and Nicholas R. Jennings. "Trust in multi-agent systems." The Knowledge Engineering Review 19.01 (2004): 1-25.

[4]. Jøsang, Audun, Ross Hayward, and Simon Pope. "Trust network analysis with subjective logic." Proceedings of the 29th Australasian Computer Science Conference-Volume 48. Australian Computer Society, Inc., 2006.

[5]. Simon, Gyula, et al. "Sensor network-based countersniper system." Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004.

[6]. Tolle, Gilman, et al. "A macroscope in the redwoods." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.

[7]. Gambetta, Diego. "Can we trust trust." Trust: Making and breaking cooperative relations 2000 (2000): 213-237.

[8]. Yap, Kok-Kiong, Vikram Srinivasan, and Mehul Motani. "MAX: human-centric search of the physical world." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.

[9]. Huang, Jyh-How, Saqib Amjad, and Shivakant Mishra. "Cenwits: a sensor-based loosely coupled search and rescue system using witnesses." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.

[10]. Werner-Allen, Geoffrey, et al. "Deploying a wireless sensor network on an active volcano." Internet Computing, IEEE 10.2 (2006): 18-25.

[11]. Zhang, Pei, et al. "Hardware design experiences in ZebraNet." Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004.

[12]. Song, Fei, and Baohua Zhao. "Trust-based LEACH protocol for wireless sensor networks." Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on. Vol. 1. IEEE, 2008.

[13]. Ganeriwal, Saurabh, Laura K. Balzano, and Mani B. Srivastava. "Reputation-based framework for high integrity sensor networks." ACM Transactions on Sensor Networks (TOSN) 4.3 (2008): 15.

[14]. Boukerche, Azzedine, and Xu Li. "An agent-based trust and reputation management scheme for wireless sensor networks." Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE. Vol. 3. IEEE, 2005.

[15]. Wu, Guowei, et al. "A dynamic trust model exploiting the time slice in WSNs." Soft Computing 18.9 (2014): 1829-1840.

[16]. Liu, Ke, Nael Abu-Ghazaleh, and Kyoung-Don Kang. "Location verification and trust management for resilient geographic routing." Journal of Parallel and Distributed Computing 67.2 (2007): 215-228.

[17]. Aivaloglou, Efthimia, Stefanos Gritzalis, and Charalabos Skianis. "Towards a flexible trust establishment framework for sensor networks." Telecommunication Systems 35.3-4 (2007): 207-213.

[18]. Babu, Shaik Sahil, Arnab Raha, and Mrinal Kanti Naskar. "Trustworthy Route formation Algorithm for WSNs." International Journal of Computer Applications (0975–8887) 27.5 (2011).

[19]. Chen, Haiguang, et al. "Reputation-based trust in wireless sensor networks." Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on. IEEE, 2007.

[20]. Momani, Mohammad, et al. "Trust Classification in wireless sensor networks." The 8th International Symposium on DSP and Communication Systems (DSPCS'05). 2005.

[21]. Shaikh R A, Jameel H,Auriol B, Lee H, Lee S, Song Y, "Group-based trust management scheme for clustered wireless sensor networks", IEEE Transactions on Parallel and Distributed Systems, October 2009. pp 1698 – 1712.

[22]. Atakli, Idris M., et al. "Malicious node detection in wireless sensor networks using weighted trust evaluation." Proceedings of the 2008 Spring simulation multiconference. Society for Computer Simulation International, 2008.

[23]. Marchang, Ningrinla, and Rohit Datta. "Light-weight trust-based routing protocol for mobile ad hoc networks." Information Security, IET 6.2 (2012): 77-83..

[24]. Trakadas, Panagiotis, et al. "A novel flexible trust management system for heterogeneous wireless sensor networks." Autonomous Decentralized Systems, 2009. ISADS'09. International Symposium on. IEEE, 2009.

[25]. Jøsang, Audun, Roslan Ismail, and Colin Boyd. "A survey of trust and reputation systems for online service provision." Decision support systems 43.2 (2007): 618-644..

[26]. Sun, Yan Lindsay, et al. "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks." INFOCOM. Vol. 2006. 2006.

[27]. He, Qi, Dapeng Wu, and Pradeep Khosla. "SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks." Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE. Vol. 2. IEEE, 2004.

[28]. Urpi, A., M. Bonuccelli, and Silvia Giordano. "Modelling cooperation in mobile ad hoc networks: a formal description of selfishness." WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks. 2003.

[29]. Gago, M., Rodrigo Roman, and Javier Lopez. "A survey on the applicability of trust management systems for wireless sensor networks." Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on. IEEE, 2007

[30]. Zeng, Zhiwen, et al. "Trust Path-Searching Algorithm Based on PSO." Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for. IEEE, 2008.

[31]. Ding, Xiajun, Xiaodan Jiang, and Shuangxia Han. "Optimization of LEACH Protocol and Environmental Monitor System Design based on WSN." International Journal of Future Generation Communication and Networking 7.2 (2014): 9-20.

[32]. Crosby, Garth V., and Niki Pissinou. "Cluster-based reputation and trust for wireless sensor networks." Consumer Communications and Networking Conference. 2007.

[33]. S. Biswas, P. Dey, and S. Neogy, "Trusted checkpointing based on ant colony optimization in MANET," Proc. - 2012 3rd Int. Conf. Emerg. Appl. Inf. Technol. EAIT 2012, pp. 433–438, 2012.

[34]. Raina, Anshuli, and Shonak Bansal. "Hybrid PSO based Leach Algorithm for Reducing Energy Consumption in Wireless Sensor Networks." International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1,2014.

[35]. Goncalo Pereira(2010, Mar), Particle Swarm Optimization(PSO), http://web.ist.utl.pt/gdgp/VA/pso.htm ( 29,May,2015)

## List of Publications

Monia, Sushma Jain, Sukhchandan Randhawa, " An Efficient Trust Management algorithm in Wireless Sensor Network", *Third International Conference on Emerging Research in Computing, Information, Communication and Applications.* Springer -2015

**Video Link**: https://youtu.be/WWuur4btF4Q