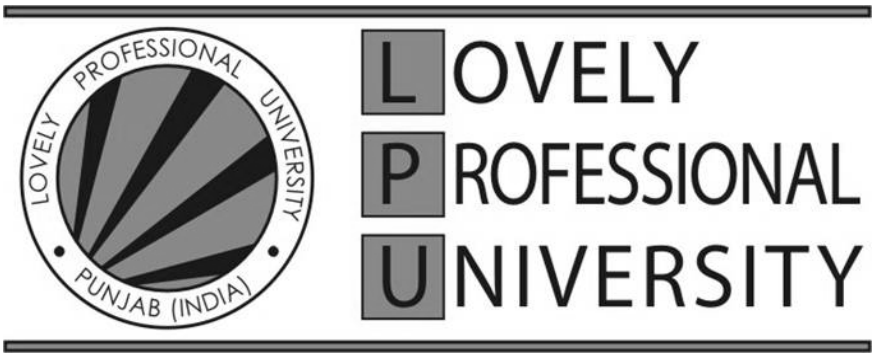


KS Algorithm: A Preventive Mechanism to avoid Intrusion in Area Monitoring Applications

A Dissertation submitted

By

KAUSHAL KISHOR JOSHI

to

Department of

Computer Science and Engineering

In partial fulfilment of the Requirement for the

Award of the Degree of

Master of Technology

In

Computer Science and Engineering

Under the guidance of

Mr. Amritpal Singh

Asst. Professor

(May 2015)

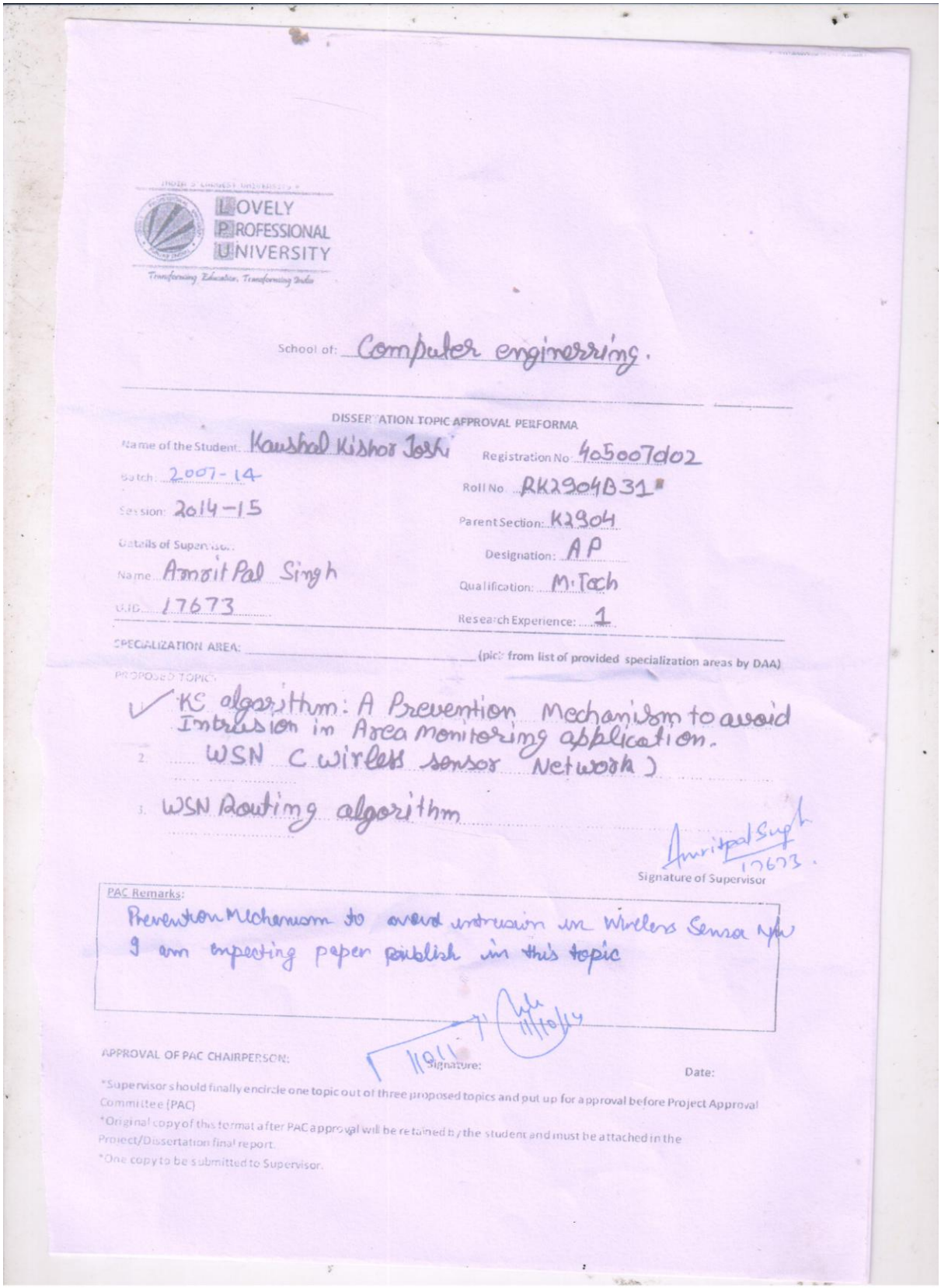
CERTIFICATE

This is to certify that **Kaushal Kishor joshi** has completed M.Tech dissertation titled **KS Algorithm: A Preventive Mechanism to avoid Intrusion in Area Monitoring Applications** under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma. The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engineering.

Date:_____ Signature of Advisor

Name:
UID

PAC APPROVAL



LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of: Computer engineering.

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: Kaushal Kishor Joshi Registration No: 405007d02

Batch: 2007-14 Roll No: RK2904B31

Session: 2014-15 Parent Section: K2904

Details of Supervisor:

Name: Amrit Pal Singh Designation: AP

U.ID: 17673 Qualification: M.Tech

Research Experience: 1

SPECIALIZATION AREA: _____ (pick from list of provided specialization areas by DAA)

PROPOSED TOPIC:

1. ✓ KC algorithm: A Prevention Mechanism to avoid Intrusion in Area Monitoring application.
2. WSN (wirless sensor Network)
3. WSN Routing algorithm

Amritpal Singh
17673.
Signature of Supervisor

PAC Remarks:

Prevention Mechanism to avoid intrusion in Wireless Sensor N/w
I am expecting paper publish in this topic

APPROVAL OF PAC CHAIRPERSON: Signature: Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

DECLARATION

I hereby declare that the dissertation entitled, **"KS Algorithm: A Preventive Mechanism to avoid Intrusion in Area Monitoring Applications"** submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Investigator
Regn. No

ABSTRACT

Sensor networks now-a-days have wider applicability in various areas whether it is deployment in hostile environments for health monitoring or area is monitoring applications. Although the literature has reviewed lots of path selection techniques, this paper provides a model for the analysis of unwanted movement in a confidential area. The proposed model cost effective and also provide a prevention mechanism from intruder attacks in data transmission process.

ACKNOWLEGMENT

I would like to place on record my deep sense of gratitude of Assistant Professor Amritpal Singh, School of Computer Science, Lovely Professional University, Phagwara, India for her generous guidance, help and useful suggestions. I wish to extend my thanks to Head of Department Dalwinder Singh, School of Computer Science for his constructive suggestions to improve the quality of this research work.I am extremely thankful to Head of School Amandeep Nagpal, School of Computer Science Lovely Professional University for providing me infrastructural facilities to work within, without which this work would not have been possible.

Kaushal Kishor Joshi

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

Wireless Sensor Networks

A wireless sensor network is a network which consists of small distributed autonomous device using sensor for monitoring the physical or environmental conditions or in other words wireless sensor network is combine sensing, communication and computing into a single small device. It is a collection of nodes organized in the corporative word where each node consists of processing capability which may contain multiple type of memory like program, data and flash, and have a power source also.

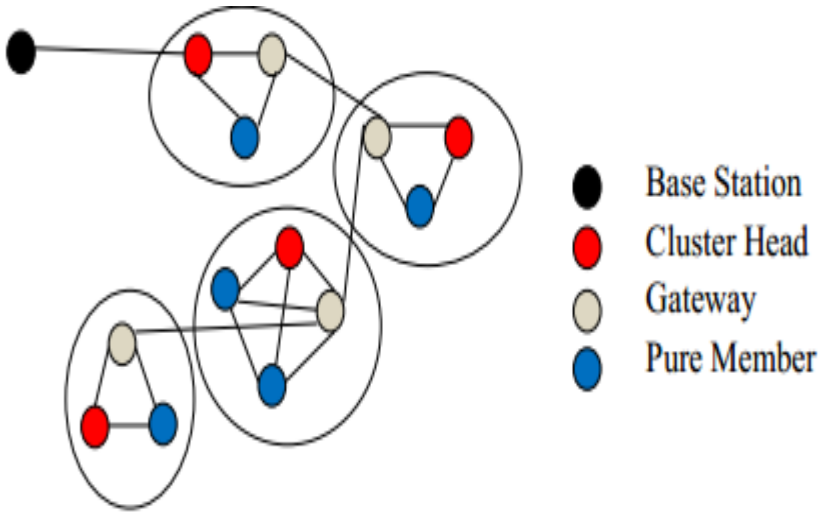


Figure 1.1 Dynamic Cluster-Based Wireless Sensor Network

A WSN in corporate is a gateway which provides connectivity back to the wired world and distributed nodes .In this network we use different types of protocols. But the protocols which we select depends on the requirements of our application .Such standard are available which includes 2.4 GHz radio based on either IEEE 802.15.4 or IEEE 802.11(is a Wi-Fi standard) .

1.1 .Applications of WSN

There are several areas where WSN is being used.

1.1.1Health Care

In this area sensors are used in utilities and remote monitoring. In this Wireless device makes less invasive monitoring and provide health care possibility. This application can be of two

types named as wearable and implemented. Wearable devices are used on the body surface of a human or closer proximity to the user and second type of devices are those devices that are inserted into the human body to sense the inner part of body and there movements. There are many other application too like body measurement and location of the person.

1.1.2 Area Monitoring

Area monitoring is also one of the commonly used applications of WSN .In area monitoring. Sensors are deployed over a region or area where some phenomenon or activity is to be monitored as in army or military bases they use sensor devices to detect the enemy intrusion or interruption. In day-to-day life a common example includes building fire detection system, geo-fencing of jails or schools attendance zones etc.

1.1.3 Air Pollution Monitoring

Wireless sensor are deployed in big cities to monitor the concentration of dangerous or harmful gases for citizen. This ad hoc wireless links are good to use rather than wired installation, this provides more mobility for testing in different area.

1.1.4 Forest Fire Detection

It is one of the useful application of the real word. Sensing nodes can be installed in forest to detect the starting point of the fire and these nodes can be equipped with sensors to measure the temperature produced in the tree by the fire and the humidity in the atmosphere. By this application fire brigade unit will be able to know when and where the fire started and how it is spreading.

1.1.5 Water Quality Monitoring

Water quality monitoring involves analyzing water properties in rivers, lakes, Demand Ocean and as well as underground water reserves. In this task wireless sensor enable the creation of a more accurate map of water status and this function allows permanent deployment station in location of difficult access without the need of manual data retrieval. There are some more application also present like “machine health monitoring (MHM)” for machine condition Based Maintenance.

1.2 Sensor

In normal electrical language “Sensor is converter that measure a physical quantity and converts it into a signal which can be read by an observer or by an instrument”. In WSN language, “Sensors are hardware devices that produce a measurable response to a change in

physical condition like temperature and pressure". Sensor produces an analogue signal which is converted to (analog-to-digital covert device) digital and then forwarded for processing to the controller.

A sensor node must have these qualities:

• Sensor node should be a smaller size device.

• Sensor node should be consuming extremely low energy.

• Sensor operates in high volume density.

• Should be autonomous and operate unattended.

• Sensor nature should be adaptive by the environment.

1.3 WSN Topologies

WSN node is normally formed in three types of topologies structure.

- Star
- Cluster Tree
- Mesh

1.3.1 Star Topologies

As the name suggest in star topologies all the node are directly connected to a common gateway.

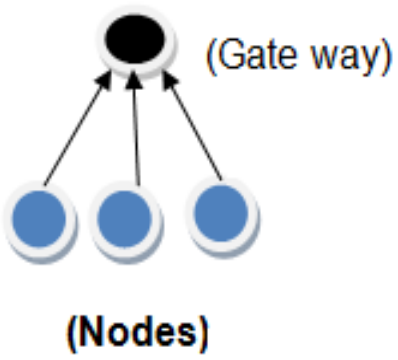


Figure 1.2 Star Topologies

1.3.2 Cluster Topologies

In cluster tree topologies each node connected to its root node or higher node and then this node is further connected to the gateway. In this data routing starts from the lowest node of the tree and go towards the gateway.

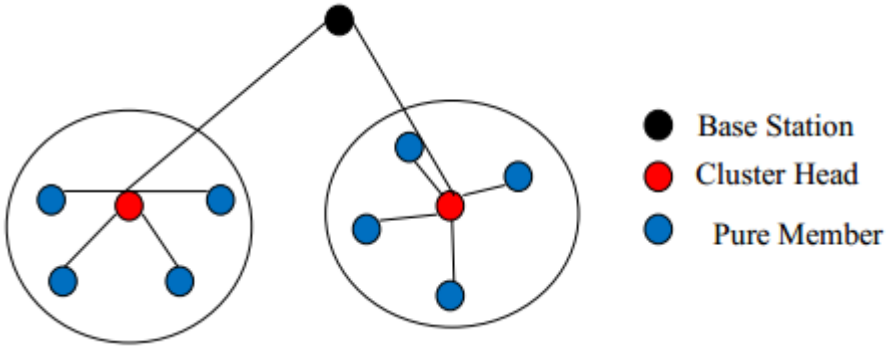


Figure 1.3 Cluster Tree

1.3.3 Mesh Topologies

Mesh topologies is most efficient topologies and provide more reliability in this network a node is connected to the multiple node, pass the data through the available path which is more reliable.

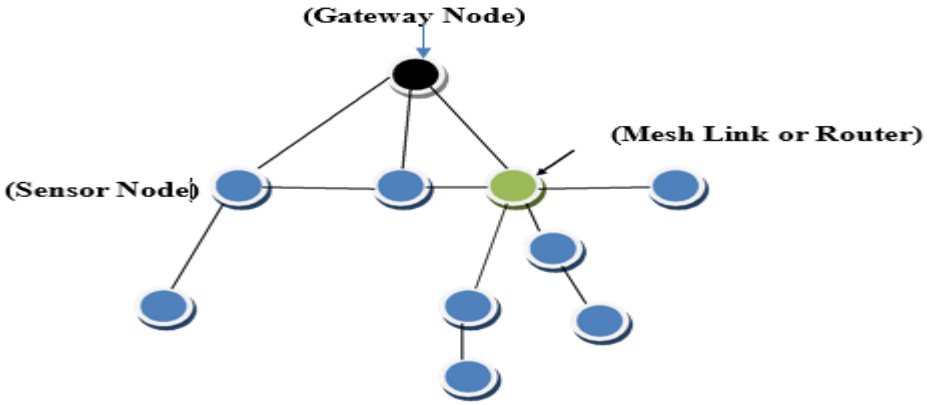


Figure 1.4 Mesh Topologies

In the above figure, Black node represents gateway, Blue node represents sensor node and Green node represents mesh link (mesh link is usually referred as a router).

1.4 Some of the challenges in WSN

- Scalability
- Heterogeneity
- Systematic Design
- Privacy and Security
- Energy Efficiency
- Responsiveness
- Robustness
- Self-Configuration and Adaptation

1.5 Trust Factor in Different Domains

The trust is the most important thing in today's world. If there is no trust, there is no relationship. Building trust is really essential. Trust helps in building stronger and reliable relationship. In case of sensor networks also building trust is really essential. If trust is not there then there could not be reliability that the node will send the data to the destination.

1.5.1 Trust in Social Science and Ecommerce

Social Science deals with the relationship between individuals in the society. Man is a social animal. He lives in a group. An individual cannot be alone for a longer span of time. He needs someone with whom he can share his thoughts. For any relationship the trust plays an important part. If there is no trust then there will be no relationship. The relationships are built on the trust.

Ecommerce means shopping online. It is purchase of items through internet. A user who purchases something online must have trust on the website he is using. If he has no trust then he will not share his bank details with the website. There are multiple online shopping websites these days. But only few are the most favorable of the clients. This is because these website have been able to build trust over a period of time.

1.5.2 Trust in Distributed and Peer-to-Peer Systems

In distributed and Peer- to-Peer systems there is no centralized entity through which the transmission could be made secure. So in these systems users keep a track on their peer nodes. If some suspicious activity is observed then the node is not considered for the data transmission. If the entity is able to build the trust then entity is used for the data

transmission. Each user records the activity performed by its peers. This trust value can be shared between different entities of the system in order to develop secure system.

Trust could be developed using reputation-based management system, by exchanging protocols revoke and refresh recommendations and Bayesian networks.

1.5.3 Trust in Ad-Hoc Networks

In Ad-Hoc Networks hubs join and leave the system all the time. Trust administration in the event of MANETS is fundamental and troublesome. The hubs in the MANETS change their position now and again. So trust of a hub is figured on the premise of its past record and the present development of the hub.

It is accepted that the bunch head is constantly genuine and it confirms alternate hubs joining the group. The bunch head completes this work with the assistance of Zero Knowledge Protocol or it could verify alternate hubs on the premise of trust level. That it if m out of n such that m>n/2 hubs concurs that a hub is validated then base station concurs it to be confirm and makes it trust level as zero. What's more, as the times passes the trust level can continue expanding. At the point when the trust level increments up to an ideal level then this hub can be picked as entryway of the bunch i.e. the movement of the group could go through this hub.

CHAPTER 2

REVIEW of LITERATURE

Bhaskar Krishnamachari (2005) presented the overview of the WSN. In this paper there is an overview of the application of the sensor network, and what are the different topologies are present in the network and which one is good. In this we get the knowledge about the different challenges which comes in the networks and give a short overview of the basic terms and application of the WSN.

Luciana Pelusi, Andrea Passarella, and Marco Conti (2006) proposed new substances of Opportunistic frameworks which is a champion amongst the most interesting investigates of MANETs. In entrepreneurial frameworks, changing center points are engaged to compare with one another paying little heed to the likelihood that it is highly unlikely that go along with them. Additionally, center points shouldn't have any data about the framework geography, which is crucial in normal guiding traditions. Courses clears a path alterably without knowing the certified association between center points. Possible center point can cunningly be used as next hop, obliged that future closer to objective center. Such essential make shrewd frameworks a test for further investigates.

(Garth V. et.al 2006), uses the trust factor in order to elect the reliable node as a cluster head. It reduces probability of selection of a compromised or malicious node as a cluster head. Therefore the cluster reliability increases. The trust factor of each node is calculated by the neighboring nodes in the cluster. At the time of election, nodes in the cluster votes for the new cluster head. The winner is declared with the simple majority. And the node having second highest votes is elected as vice cluster head. The work of vice cluster head is to act as cluster head in case the newly elected cluster head fails, before handling the control to its successor. Advantage of the above scheme is that the cluster head reliability is increased as the chances of malicious node to be elected as cluster head is reduced. Secondly the election of vice cluster head also increases the reliability of the cluster. Drawback is that the election algorithm does not include any other parameter other than the trust level. It does not take into account the energy level of the cluster head.

(Yixin Jiangand at el 2006) proposed another shared verification and key trade convention. The two principle peculiarities of this convention is personality namelessness and session key

reestablishment. This convention gives secure meandering administrations to the true blue client between the home and going to operators or so, this convention gives secure handoff to the real client [15]. The proposed convention is focused around the emit part rule and insisted toward oneself plan. The convention lives up to expectations in two stages: First stage is the common validation with secrecy which conceals the utilization's genuine character when a honest to goodness client is meandering from the home operators to the meeting specialists. This stage utilize the transient character (TID) rather than the client's genuine personality. Second stage is the session key restoration stage which restores the imparted key which is imparted between the authentic client and the serving operators.

Al-Sakib Khan Pathan (2010) talk about majority of the assaults against security in remote sensor systems are brought on by the insertion of false data by the traded off hubs inside the system. For protecting the consideration of false reports by traded off hubs, a method is needed for catching false reports. On the other hand, creating such a location system and making it effective speaks to an extraordinary exploration challenge. Once more, guaranteeing comprehensive security in remote sensor system is a real research issue. A significant number of todays proposed security plans are focused around particular system models. As there is an absence of consolidated push to take a normal model to guarantee security for each one layer, in future in spite of the fact that the In this research paper they give security components get to be entrenched for every individual layer, consolidating all the components together for making them work as a team with one another will acquire a hard research challenge. Regardless of the possibility that comprehensive security could be guaranteed for remote sensor organizes, the expense viability what's more vitality proficiency to utilize such components could in any case posture extraordinary examination n challenge in the advancing days.

(Guo Li-Qing et.al 2010), uses ACHTH-LEACH in which the cluster head is chosen on the basis of energy level which is remaining in the node and transfers the data to BS using two-hop transmission that is the data from the cluster head is not transferred directly to BS but instead it is sent to one of the cluster head which is near to BS and then this cluster head further sends it to BS [10]. This way the energy of the nodes is saved. The cluster is divided into two regions near region and far region. The cluster head in far region when wish to transfer the data to BS, it sends it to the cluster head of near region and then cluster head of near region transfers it to BS. The basic drawback being that it works on the homogenous

cluster only and in case the near cluster head is not activated then the far cluster head sends the information to the base station directly which wastes the energy of the cluster head of far region and the cluster head is being elected only on the parameter of the remaining energy of the nodes. The authentication of cluster head is not being taken care of.

Andreas Georgakopoulos, Kostas Tsagkaris, Vera Stavroulaki (2011) principally concentrates on one major issue of artful system which is system creation issue and especially this paper concentrates on the effective route for determination of hubs to take an interest in the system. This is accomplished through the definition of hub choice issue and by considering as a result of a wellness work that takes for different components of hubs. Their Characteristic results are introduced to acquire little verification for the proposed idea. This proposed idea will accomplish to its normal result through definition of the hub choice and by thought of a wellness capacity. All the Characteristic results are exhibited to increase some evidence of idea for the proposed arrangement. The coveted result will incorporates an estimation for astute system's required lifetime in agreement to their re-enactment results and estimation of the conveyance likelihood for variable number of hubs.

Chen xi, Tian you liang (2012) presented advancement for deferral tolerant systems and versatile specially appointed systems which is generally utilized as a part of both of nonmilitary personnel and military .Nonetheless, they have the security issues that are progressively genuine because of their characteristic attributes of being great discontinuous and being self-sorted out. In this paper, they have displayed the key issues and difficulties for pioneering systems at system layer with understanding to issues they have given security plans, for example, the key administration, security steering, and trust administration. Based upon all such talks, at last they brought up the potential future exploration limits for the security in sharp systems. In this paper, they have overviewed different sorts of security issues in entrepreneurial systems from different perspectives. It is clear that the specific attributes of crafty systems make it all the more impeccably fine despite potential assaults and dangers. The fundamental key administration instrument that can supply the essential security administrations are still difficult to be accomplished, for situation in regards to pioneering systems. As this system work in a very surprising toward oneself composed appropriated route for an amazing variable situations.

White paper titled **Routing techniques for Opportunistic Networks and Security Issues** has presented opportunistic networking which has considerable interest from the research scenario in few years. In opportunistic networks, mobile nodes are able to communicate with one another even if a route connecting each of them never exists. An opponent grows from its base to the original set of nodes employed together at the time of the initial stage. The formulation base grows into a larger network by extending invitations to join the opponent to foreign stations, nodes, or networks that it is able to join. The design methodology of reliable routing techniques for opportunistic networks is usually a big challenge. In this paper, they survey the various routing algorithms for the opportunistic networks as well as they discuss the security aspect for the opportunistic networks.

(R. Pre ma1, R. Rangarajan at el 2012) talk about remote sensor system applications should choose the inborn change between vitality effective communication and the necessity to accomplish favored nature of administration (QoS, for example, bundle conveyance degree, delay and to decrease the force utilization of remote sensor hubs Keeping in mind the end goal to address this test, they propose the Force Mindful Steering Convention (PARP), which achieves application-defined correspondence delays at low vitality cost by alertly adjusting transmission power and directing choices. Broad recreation results demonstrate that the proposed PARP accomplishes better QoS and diminished force utilization.

(Suvadip Batabyal, Parama Bhaumik at el 2012) they have attempted to discover the effect of RWP (Arbitrary Waypoint) versatility over bundle conveyance proportion. They gauge numerous portability variables like number of hub contact duration(link time) and the last is between contact time which further relies on a few parameters like aggregate system region, number of hubs, hub speed and radio recurrence scope of the hubs. They have likewise proposed a limited structure for RWP versatility model, which they called the partiality based portability model. The proposed system situation comprises of one source and one objective hub which are put at two distinctive great corners of the aggregate system region (in order to give greatest separation between them). All the correspondence and trading of information parcels is finished with the assistance of versatile "partner" hubs. Thus the source hub and the end of the line hub are altered and can’t move. The portable hubs help in exchanging the message. Henceforth, they proposed a gullible proclivity based portability model.

(Swimpy Pahuja at el 2012) proposed a new algorithm in which they found an alternative routing path for each data transmission call to overcome the network attack. This increased the network reliability. The algorithm allowed sensor data base to be sent on defined routing path using various transmission modes. This algorithm used to transmit sensory data over the network with the secure mode. This algorithm provide prevention mechanism in which if any node failure or congestion on existing shortest path occurs, then a secure alternative path is been established for routing sensor data over wireless sensor network.

(Swimpy Pahuja at el 2012) basically discuss abut RFID (Radio frequency identification).RIFD mainly work on various attack and problem prevention widespread .In this research paper the researcher focused on designing a secure and efficient protocols for authentication between tag and reader in RFID system .They designed a scalable and untraceable protocols to provide data integrity and security . In this protocol T needs four hash operation to communicate with the R which is provide quite good security.

CHAPTER 3

PRESENT WORK

3.1 Scope and Study

3.1.1Network security

There is some base question which comes to mind

- Why we need security in WSN
- IS security is possible in sensors.
- Than what are the requirements.

3.1.1.1 Why we need security

As per we know in today's worlds there are lots of transition of data, money important information is done by the medium of wireless networks. So to providing the security to this network means to make them more flexible, reliable and safe so as to prevent the data to pass out or leak since there are lots of hackers in this world who tries to misuse this type of data in wrong way.

3.1.1.2 Security is Possible

We can apply some of security algorithm on the sensor node to provide the security on transition. A particular challenge is broadcasting authenticated data to the entire sensor network. Current proposals for authenticated broad-cast are impractical for sensor networks.

3.1.1.3 What is requirement?

Here are some aspect that why we need security.

3.1.1.3.1 Data Confidentiality

Data confidentiality is one of the main task of sensor to not pass or leak, sensor reading or data to near networks. Sensor node communicate in such application also in which the data is very sensitive like an example of key distribution, for that keeping data safe we use data encryption with a secret key which only receiver know or possess ,and through this provide data confidentiality.

3.1.1.3.2 Data Authentication

Message authentication is one of the important tasks for the lots of application in sensor network. When we are using sensor network, data authentication is necessary for many administrative tasks. Since an attacker can easily inject any intuition message in this sensing network. So the receiver needs to be sure that message is coming from a trusted source if any message is about personal information like in e-banking pattern.

There are two type of key distribution mechanism through which data authentication can be achieved. First one is known as a pure symmetric mechanism. In this sender and receiver share a secrete key to get MAC (Message Authentication code) of all communicated data by computing. But the drawback or limitation is that it can't be used for broadcast setting. So for the authentication in broadcasting we use asymmetric mechanism.

3.1.1.3.3 Data Integrity

In correspondence, information respectability guarantees the beneficiary that the got information is not adjusted in travel by a foe. In SPINS, we attain to information trustworthiness through information confirmation, which is a stronger property.

3.1.3.4 Data Freshness

Given that all sensor networks is work on some type of time varying measure. And we have been insure that the message which is coming is fresh and it is not adversary replayed old messages. To identify the freshness we have two type of freshness.

a) Weak Freshness: - This provides us small or particle message but it there is no delay information in the message. It is required for a sensor measurement.

b) Strong Freshness: - It give us a total order on request –response pair, and allows for delay estimation. It is useful in the task of time Synchronization with the network

3.2Problem Formulation

WSN had become the most popular choice for area monitoring. Many types of sensor nodes are available for monitoring the area like seismic sensors, image sensor, thermal sensor etc. WSN is the most economical method for area monitoring due to which the technique has been adopted by different countries. Use of sensors for this purpose had reduced the cost of monitoring. Also, the no of solder and chopper needed to monitor the area for providing security has been reduced. Thus, security factor has been compromised to some extent. Now, the intruder can easily sense the information being transmitted about an area and he can change it also very easily. As an example in military areas or attack-prone areas, it becomes a necessity to get the correct information about an area as a little change in the received information can prove dangerous for the country. Therefore, the paper provides a preventive mechanism against this man-in-the-middle attack so that this confidential information about an area should reach the concerned officials safely and we would be able to prevent the area from accidents.

3.2.1Working of the system:-

For the area monitoring today we used different types of sensor nodes to deploy together for gathering more efficient data and accurate data [16]. A wireless sensor network consist large no of sensor nodes to deploy in the area which is to be observed. These nodes are deployed in random topology to cover the area. Sensor has low power battery and low range. So it can‟t send data to the process node directly. Therefore, information is transferred by multi hop path to sink node and the data can be send any kind of abstract alarm or aggregated data to base station.

3.2.2Challenges or issues: -

The are many challenges in critical mission like border monitoring

a) Energy Efficiency: - Area monitoring is a confidential task. In this the position of deployment of sensor nodes has to be kept confidential. So in this area changing the battery of a node manually is not a practical or possible task. So it is a great challenge to create energy efficient node. Although some solar power nodes came into existence in the literature but they are also inefficient.

b) Quality of service: - QOS is one of the main issues. The monitoring should be reliable to detect the intrusion and communication between sensor and sink node must be fast, there should not be any kind of delay.

c) Quality of coverage: - To cover the area of monitoring field the deployment of sensor should be in best place.

e) Security Issue: - In area monitoring the major task of sensor node is to send the data confidentially to the destination. Data should be encrypted, secured and protected against any attack.

Many types of attacks are possible while data transmission. But most common attack out of them is man-in-the-middle attack. Whenever an intruder tries to attack, it's not an easy task to trace all the routes so instead of tracing all paths it follows a pattern. Usually the intruder follows or selects the shortest path for attack. In man-in-the-middle attack intruder is capable of monitoring all the data which is transmitting over the network. He is also capable of inserting any message to change the monitor data or add any wrong information. The attack can be at any node in the path so it's hard to stop that

3.3 OBJECTIVE

The goal of this thesis is to do the study of sensor security and analysis their behavior on different parameter and try to implement a prevention algorithm in the field of area monitoring of the algorithm. And do a comparative study on their behavior.

To achieve the above defined objective we can propose one of the proposed routing algorithm implementation known as “KS algorithm”.

Implemented model as the interruption while data transmission is a big issue in area monitoring which poses a great effect on data confidentiality. A prevention mechanism has been proposed with the help of an routing algorithm named as “KS Algorithm “, to reduce the probability of attacks [10] while data is transmitted. This new algorithm provides a method for computation of an alternative path. In order to prevent the confidential data from man-in-the-middle attack. Path computed may not be shortest one and would not include any node from the shortest path which is more prone to intruder attack. In this algorithm, a node would communicate to other node only if that node is authenticated or declared safe node.

3.4 Research Methodology

This algorithm involves some assumption

a) Source node has the information of residual battery power, cost to send data as well as minimum distance to be covered for all the nodes in particular area.

b) There is some mechanism named as automatic update mechanism. Which keeps on updating the information of others node to the source node.

c) There is no transmission delay while transmitting the message.

In this algorithm we consider alternative path on some parameter Low power consumption: the power consumption must be low

a) Maximum power battery: - the node which we selected, there power of battery must be high.

b) Minimum cost: - the cost of transmission along path should be as minimum as possible.

Flowchart of proposed methodology

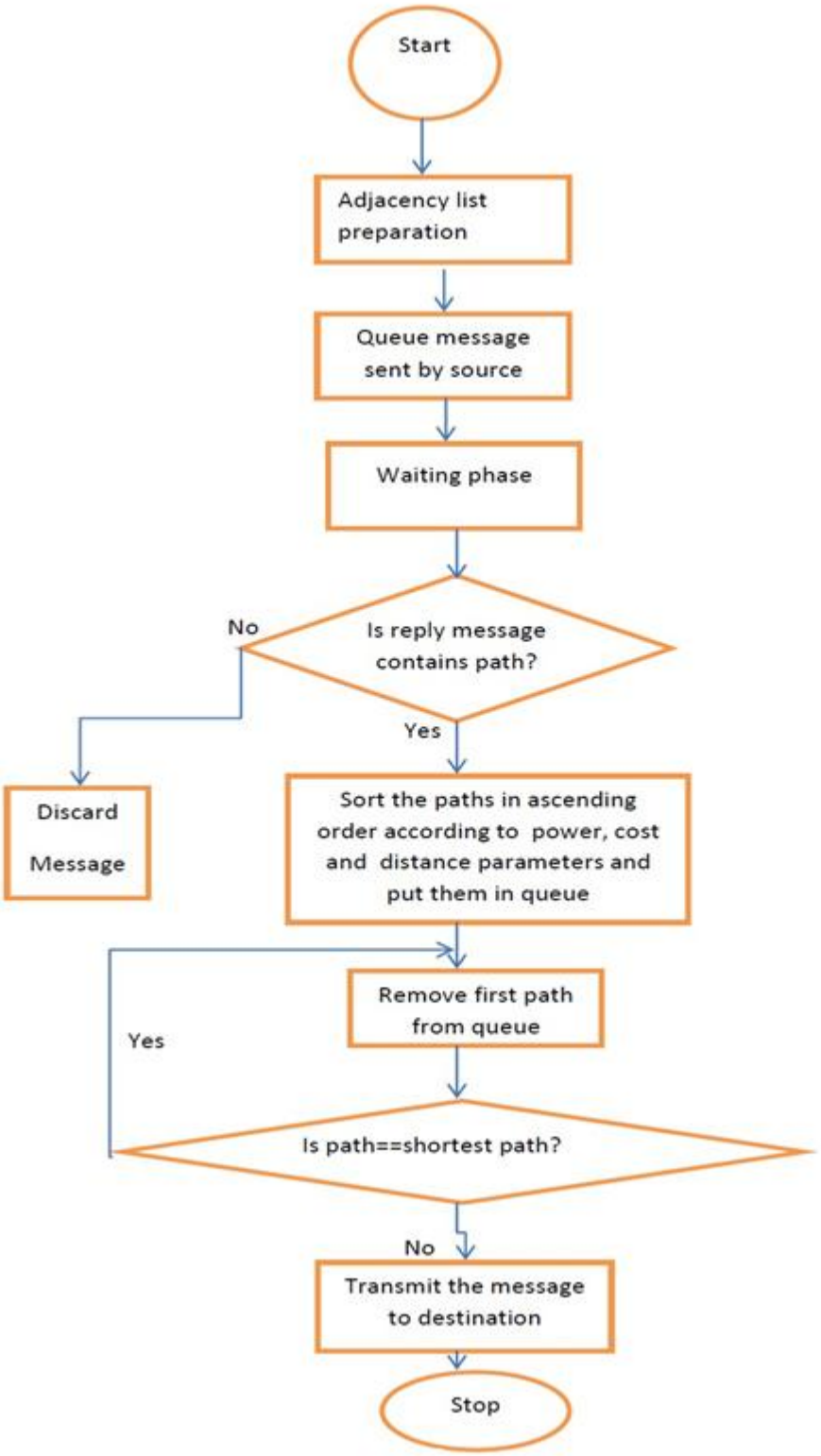


Figure 3.1: Flow diagram

Basically the algorithm works five different phases.

a) **Adjacency list preparation**: - in this phase each node prepare there its adjacency list i.e. each node find the list of all its neighbor through which data can be sent.

b) **Message sending phase** :- in this phase source node send an query message or in this algorithm we can call as help message too, to all its nodes which is present into the adjacency list .like ((A0,D0)(A1,D1)……..(An,Dn)).

c) **Wait phase** :- in this phase on receiving query message or „help" message, each node prepare its reply message with containing cost and power of the path from the destination in terms of "K" value .

Calculation of "K" value

The "K" factor is calculated in in three steps:-

1. Calculation of C (t):- In this we calculate the transmission cost, which is been calculated by the following equation.

$$C(t) = T(\text{hop count}) \quad \ldots\ldots\ldots\ldots\ldots (1)$$

In this T is and predefine standard cost which is define by the use on per unit distance and t is time taken in transmission. The total cost of it C (t) in multiplication of the standard distance cost and time taken in it.

2. Power of battery (P):- second factor in power of battery which we take in as
Factor Pdf. Pdf is known as a packet discretion factor

$$\text{Power of battery of node} = -\text{Pfd} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

3. K" factor: - In the end by calculation all the values now we calculate the K factor by putting the value in equation K=min (-) pdf && min (-) hop count.

In this equation (-) sign show that cost must be less than power for the transmission successfully. And in this transmission will be ideal when cost will be minimum and battery power of node will be maximum.

So after calculating the K factor of all the nodes the node reply there message with the parameter value of K.

(d) **Path selection phase**:- in this phase after getting the reply of possible path with k values from all the nodes, source node select the best path based on parameter pdf, hop count and seq no it has with it .

e) **Transmission Phase: -** Now the information is been transmitted through the securely calculated alternative path.

This algorithm provides us different advantage.

- Its provide us a prevention mechanism by selecting the alternative path which in not follow any fixed pattern so it reduce the probability to attack on a node while transmission the message. Along with that we can use if any intruder do an attack on suppose transmission, but next time he do again the same path will be changed. So he will find another node Which will give us time to find that attacker .Or as we now maximum battery power is a priority in the path selection we can use any node of maximum power as an honey pot or a trap for the intruder. So we can catch if any attack happed.
- **Power Balancing**: - As we know this algorithm chose node on maximum power battery. So it provide us distributed power load mechanism. So its avoid the dead node case of any sensor because cannot take any node who have battery value less than 10.
- **Cost effective**: As we see its chose the minimum cost nodes while transition so provide us cost effective approach.

3.5 Dependency of Different File in KAODV:-

KAODV is a routing protocol so different agent in this derived from different. Class agents file. Dependency of the different class file is shown below.

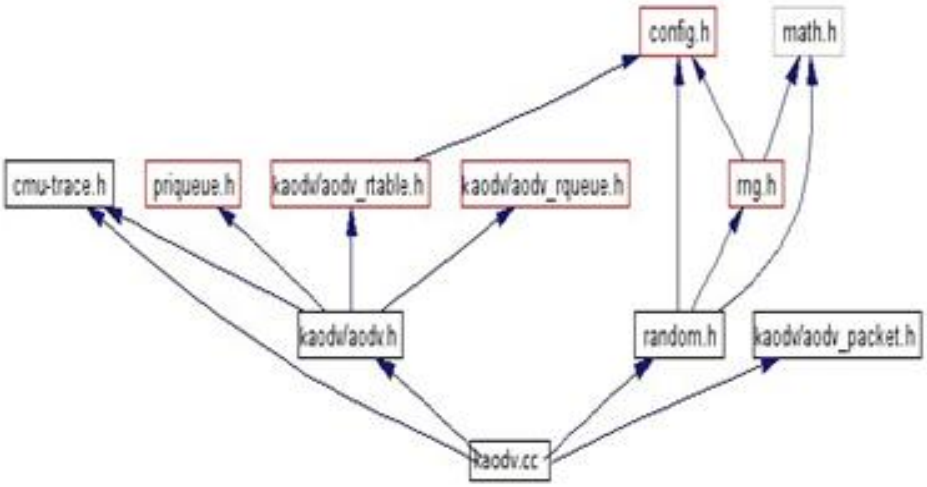


Figure3.2 File dependency of kAODV.cc

3.5.1 The Normal Flow of the kAODV

1. When user select KAODV as an routing protocol through this command

$ns node-config-adhoc Routing kAODV

Then the pointer move in start function and then this start function move the command function kAODV protocol.

The command function has two type of timer in "start" which is name as

htimer.handle((event)0);

btimer.handle((event)0);

2. So after that if h timer is working then flow move to hello Timer::handle (event*) function and its shown in the lines below

agent -> sendHello()

double interval = MinHelloInterval + ((MaxHelloInterval - Min-HelloInterval) * Random::uniform()); assert(interval->=0); Scheduler::instance().schedule(this, &intr, interval);

This code ca l‟s the sendHello() function by configuring there interval of hello packets .

3. So now pointer come to the KAODV:sendHello() function and then move towards the scheduler::instance.sehedule(target_p,0.0),whose functionality is to schedule packets.

4. In the goal node KAODV::rec(packet*p,handler*) function is called but this process is done after receiving a packet by the node.

5. After the reeckAODV(p)function is call kAODV::recv(packet*p,handler)function After the reeckAODV(p) function is called by the kAODV::recv(packet*p,handler)function.

6. After this kAODV::recKADOV(packet*p)function check the different packet types and then call there respective functions.

7. At the end recvhello()function is called

TRACE FORMATE OF KAODv:-The format of the trace file np1.tr Is contains this values :-

Column-Number	What Happened	Value of this instance
1	It shows the occurred event	's'SEND, 'r' RECEIVED, 'D'DROPPED
2	Time at which the event occured?	12.000000000
3	Node at which the event occured?	Node id 0
4	Layer at which the event occured?	AGT' application layer, 'RTR' routing layer,'LL' link layer, 'IFQ' Interface queue, 'MAC'mac layer, 'PHY' physical layer
5	Show flags	----
6	shows the sequence number of packets	0
7	shows the packet type	cbr' CBR packet, 'DSR' DSR packet, 'RTS'RTS packet generated by MAC layer, 'ARP'link layer ARP packet.
8	shows size of the packet	Packet size increases when a packet moves from an upper layer to a lower layer and decreases when a packet moves from a lower layer to an upper layer
9	[....]	It shows information about packet, duration,mac address of destination, the mac address of source, and the mac type of the packet body.
10	show flags	----
11	[....]	It indicates data about source hub ip : port number, goal hub ip: port number, ip header ttl, and ip of next bounce

Table 3.1 Trace format

3.5.2 Explaining Functions of File kAODV.cc and KAODV.h

Hello packets are disable by default in kAODV

if AODV LINK LAYER DETECTION

endif LINK LAYER DETECTION and recompile ns2 by using the following commands on the terminal

- make clean
- make
- sudo make install #

By this two code lines which is present in kaodv.cc we enable this process.

3.5.2.1 Timer which we used: - it is used to trigger a particular type to action of example hello packet time interval.

There are different timer which is used

```
/
  Timers (Broadcast ID, Hello, Neighbor Cache, Route Cache)
*/
class kBroadcastTimer : public Handler {
 public:
        kBroadcastTimer(kAODV* a) : agent(a) {}
        void    handle(Event*);
 private:
        kAODV    *agent;
        Event   intr;
};

class kHelloTimer : public Handler {
 public:
        kHelloTimer(kAODV* a) : agent(a) {}
        void    handle(Event*);
 private:
        kAODV    *agent;
        Event   intr;
};

class kNeighborTimer : public Handler {
 public:
        kNeighborTimer(kAODV* a) : agent(a) {}
        void    handle(Event*);
 private:
        kAODV    *agent;
        Event   intr;
};
```

Figure 3.3 Agent handler and hello packet broadcasting

```
ass kRouteCacheTimer : public Handler {
ublic:
        kRouteCacheTimer(kAODV* a) : agent(a) {}
        void    handle(Event*);
rivate:
        kAODV    *agent;
        Event   intr;

ass kLocalRepairTimer : public Handler {
ublic:
        kLocalRepairTimer(kAODV* a) : agent(a) {}
        void    handle(Event*);
rivate:
        kAODV    *agent;
        Event   intr;
```

Figure 3.4 Request root handler

a) Broadcast Timer : work of this timer is cleaning ID's of neighbor node and schedule after BCACI_ID_SAVE.

b) Neighbor Timer: Its function is to clean the neighbor entry those are time out.

c) Hello Timer:-its work is to send the hello packet to maintain delay time equal to the interval time.

d) Local Repair time: - Its work is to repair the down or broken route

e) Route Cache Timer: - It clean the route from the routing table and schedule after the every frequency

3.5.2.2 General Functions

a) Void recv (packet*p,handles*): at network layer packet firstly received at recv() function, which is sent by the mac layer in up direction

The recv() :- it checks the packet type if the packet type is aodv. It will decrease TTL and call recKAODV() function if the node generating its self then add ip address to handle broadcasting , else check the routing loop if routing loop is present the Drop the packet ,otherwise forward.

b) Int Command (int,const.char*const*): Every object created in ns-2 establisher an instance procedure, cmd{} as a look to executing method then.

3.5.2.3 Function for routing table management

```
        /*
         * Route Table Management
         */
        void            rt_resolve(Packet *p);
        void            rt_update(kaodv_rt_entry *rt, u_int32_t seqnum,
                                  u_int16_t metric, nsaddr_t nexthop,
                                  double expire_time);
        void            rt_down(kaodv_rt_entry *rt);
        void            local_rt_repair(kaodv_rt_entry *rt, Packet *p);
public:
        void            rt_ll_failed(Packet *p);
        void            handle_link_failure(nsaddr_t id);
protected:
        void            rt_purge(void);

        void            enque(kaodv_rt_entry *rt, Packet *p);
        Packet*         deque(kaodv_rt_entry *rt);
```

Figure 3.5 Route table management

1. Void rt_resolve (packet*p): This work first set the transmit disappointment get back to and afterward forward the bundle if the course is up else check if the hub is the source of parcel and do a course ask for else if local repair is in advance the cradle the parcel. In the event that capacity found that it needs to forward bundle to another person to which it doesn't have a course then drops the parcel and course lapse are show to its neighbor.

2. Void rt update(kaodv rt entry*rt, u int32t seq num ,u int16 t metric, ns addr next hop, double expire time):This function do the process of updating route .

3. Void rt_down(kaodv_rt_entry*rt):-its first confirms that the route note be died (down) more then once and after that down the route .

4. Void local rt repair(kaodv rt entry *rt, Packet *p):- it first buffer the packet and the route or under repair and RREQ packet by calling send request() function.

5. Void rt_II_failed(packet*p):- Basically this function is involved when the link report a failure this function drop the packet if link layer is not detect other wise ,if this found broker link as closer to the destination then source then it will try to call a local repair.

6. Void handle_linkfailure(naddss_t) :this is responsible for holding the link failure .itfirst checks the destcount.if destcount, if itis equal to the remove path nabhiour. Otherwise if des count>0 then send the error by calling send error() function, else free the packet

7.Void rt_purge(void):this function is responsible for purging routing tool .For each node it check route has expirdor not. if it found that valid route expired then it will clean all the packets from send buffer and invalid the route ,by dropping the table packets and tracing dropRTR_NO _Route n the tracefile.

8. Void enque(aodv rt entry *rt, Packet *p): Use to enqueue the packet.

9. Packet* deque(aodv rt entry *rt): Use to dequeue the packet.

3.5.3 Function for neighbor management

```
 * Neighbor Management
 */
void            nb_insert(nsaddr_t id);
kAODV_Neighbor*       nb_lookup(nsaddr_t id);
void            nb_delete(nsaddr_t id);
void            nb_purge(void);
```

Figure 3.6 Neighbor table management

- void nb insert(nsaddr t id): its is used to insert the neighbor.
- kAODV Neighbor* nb lookup(nsaddr t id): it is used to lookup the neighb
- void nb delete(nsaddr t id):it is responsible to delete the neighbor and It comes in action when a neighbor became longer reachable.
- void nb purge(void): this clean timed-out neighbor entry and It runs in a every HELLO INTERVAL * 1.5 seconds.

3.5.4 Functions for Broadcast_ID Management:

```
 * Broadcast ID Management
 */

void          id_insert(nsaddr_t id, u_int32_t bid);
bool         id_lookup(nsaddr_t id, u_int32_t bid);
void          id_purge(void);
```

Figure 3.7 Broadcast id management

- void id insert(nsaddr t id, u int32 t bid): it work on inserting the node broadcast_Id.
- bool id lookup(nsaddr t id, u int32 t bid): this function monitor broadcast ID.
- void id purge(void): this function is used to clean the broadcast ID.

1. **Functions for Packet Transmission Management**

```
 * Packet TX Routines
 */
void            forward(kaodv_rt_entry *rt, Packet *p, double delay);
void            sendHello(void);
void            sendRequest(nsaddr_t dst);

void            sendReply(nsaddr_t ipdst, u_int32_t hop_count,
                          nsaddr_t rpdst, u_int32_t rpseq,
                          u_int32_t lifetime, double timestamp);
void            sendError(Packet *p, bool jitter = true);

/*
```

Figure 3.8 Packet Transmission Routines

- void forward(aodv rt entry* rt, Packet p,double delay): this function performing forwarding the packets.
- void sendHello(void): This function perform sending the Hello messages in a broadcast fashion.
- void sendRequest(nsaddr t dst): its work is to send Request messages.
- void sendReply(nsaddr t ip dst, u int32 t hop count,nsaddr t rpdst, u int32 t rpseq,u int32 t lifetime, double timestamp) function is used to send Reply message.
- void sendError(Packet *p, bool jitter = true) its work is to send Error messages.

2. Functions for Packet Reception Management

```
 * Packet RX Routines
 */
void            recvkAODV(Packet *p);
void            recvHello(Packet *p);
void            recvRequest(Packet *p);
void            recvReply(Packet *p);
void            recvError(Packet *p);

/*
```

Figure 3.9 packet RX routine

- KAODV::recvAODV(Packet *p): It classify the type of incoming AODV packets. If they are of type RREQ, RREP, RERR, HELL then its call recvRequest(p), recvReply(p), recvError(p), and recvHello(p) functions respectively.

- KAODV::recvRequest(Packet *p):it call when node receive a request type packet .

- KAODV::recvReply(Packet *p): it calls this when node receive a reply type of packet .

- KAODV::recvError(Packet *p): it calls when node receive an ERROR message. KAODV::recvHello(Packet *p): it receive HELLO packet and search into neighbor list, if node is not there in neighbor list, It put the neighbor.

Chapter 4

RESULTS and DISCUSSION

By the implementing this algorithm we are going to discuss these results with respect to another routing protocol name as AODV.

- Delivery ratio
- Throughput
- Graph between packets lost.
- Graph Between packet delay
- Graph b/w output

4.1 Delivery Ratio: - it is the ratio of the packet which is sent and the packet which is received.

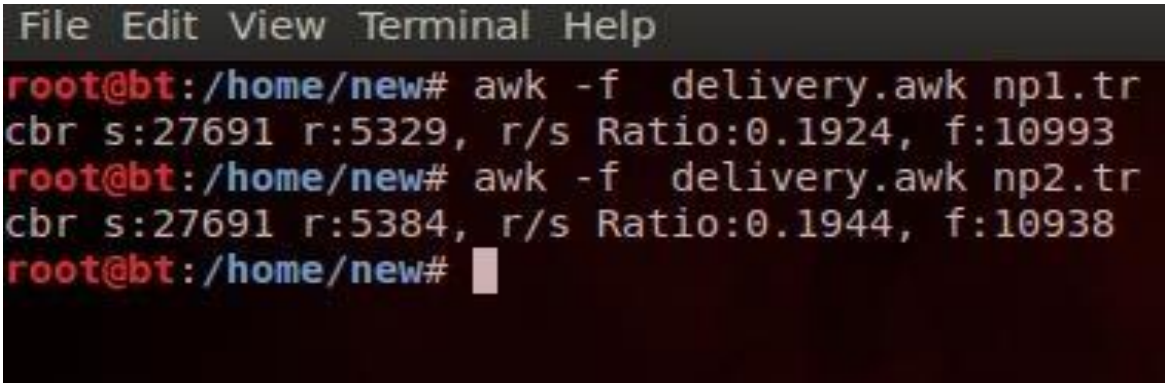


Figure 4.1 Delivery ratio of KAODV and AODV

s:=this shows the of packet send by the source

r= no of packet received by the destination node

r/s Ratio :- it's an ratio b/w receive and send packet f= it the no of packets failed .

np1:- it's for the trace file of aodv np2:- it is the trace file of kaodv

SO such as result showing the values in table below

protocol	Send packet	Receive packet	Ratio	Failed Packet
AODV	27691	5329	0.1924	10993
KAODV	27691	5384	0.1944	10938

Table 4.1 Delivery rate of KAODV is better than AODV

4.2 Throughput: - it is the average of the packets send per second.

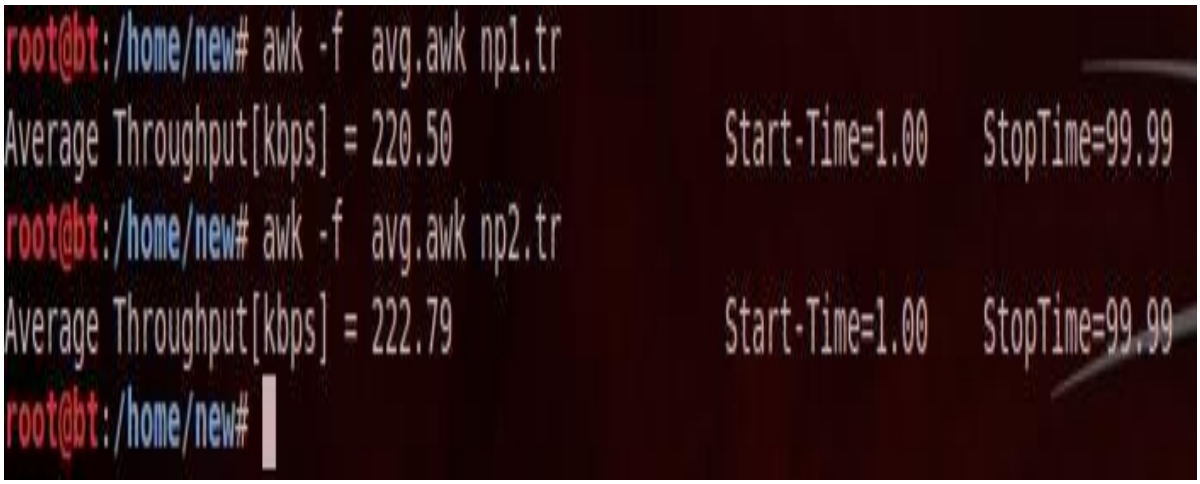


Figure 4.2 Quality of service

Start: - it's the starting time of transmission start .

Stop time= it the time when packet sending stop

Protocol	Throughput[kbps]
AODV	220.50
KAODV	222.79

Table 4.2 Throughput results

As per result is showing KAODV provides better throughput then AODV Which gives better QOS.

4.3 Graph of lost packets:-

Alost.tr is trace file of AODV protocol Klost .tr is trace file of KAODV protocol Lost graph:-

#Xgraph alost1.tr klost2.tr

As per graph showing packet lost rate between alost and klost, where alost is reprenting the graph of "aodv" algorhm and k lost is showing the packet lost graph of ks algorithm . According to the graph the ks algorithm drop or less packets as compare to the 1st aodv algorithm its saves the energy of the nodes.

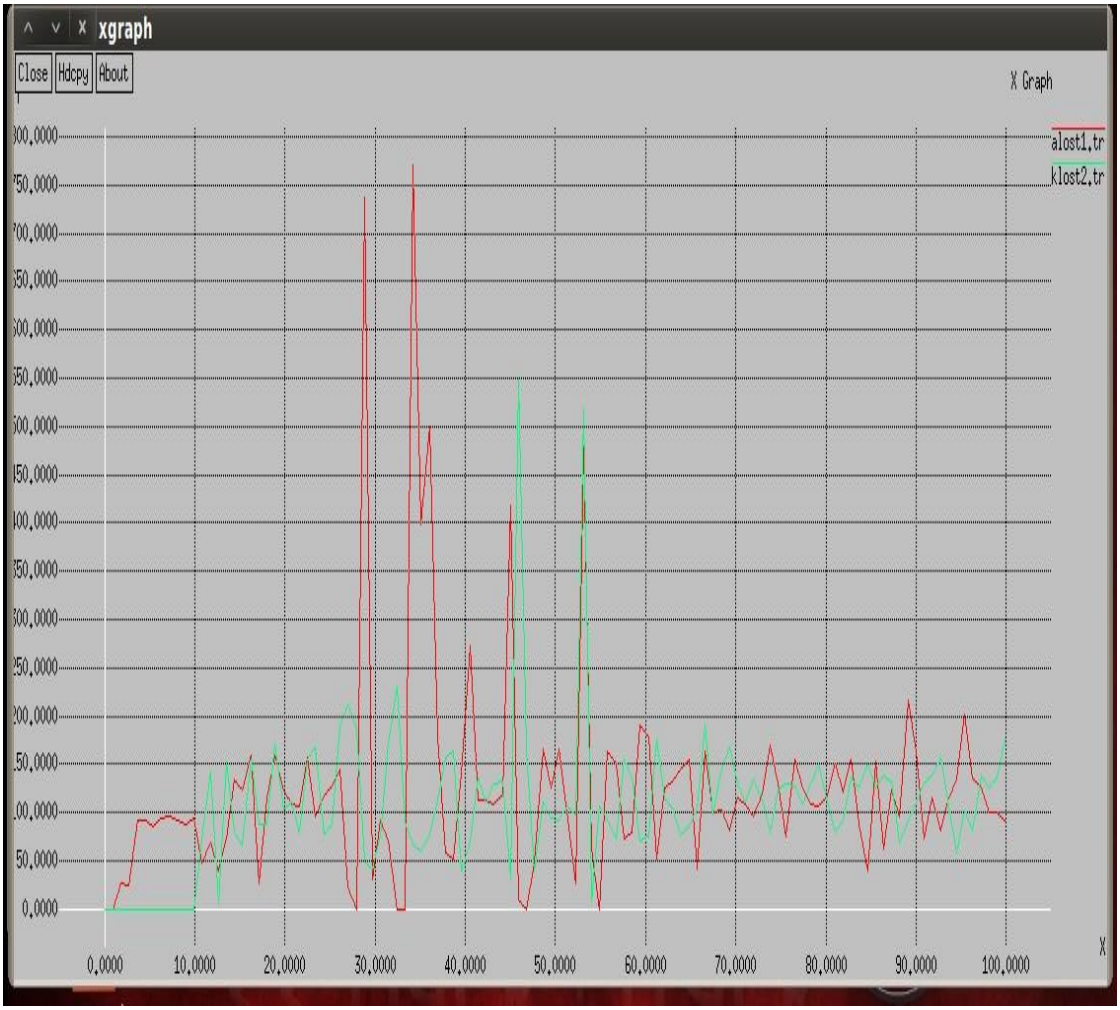


Figure 4.3 Graph of packet delivery ratio

According to this graph the packet delivery ratio of the ks algorithm is better than the aodv , which reduce the energy consummation of the sensor. And improve QOS.

4.4 Explanation of delay graph:-

 # xgraph adelay1.tr kdealy2.tr

A. As per graph showing delay rate through between adelay and kdelay ,where adelay is reprenting the graph of “aodv” algorithm and k delay is showing the delay graph of ks algorithm .

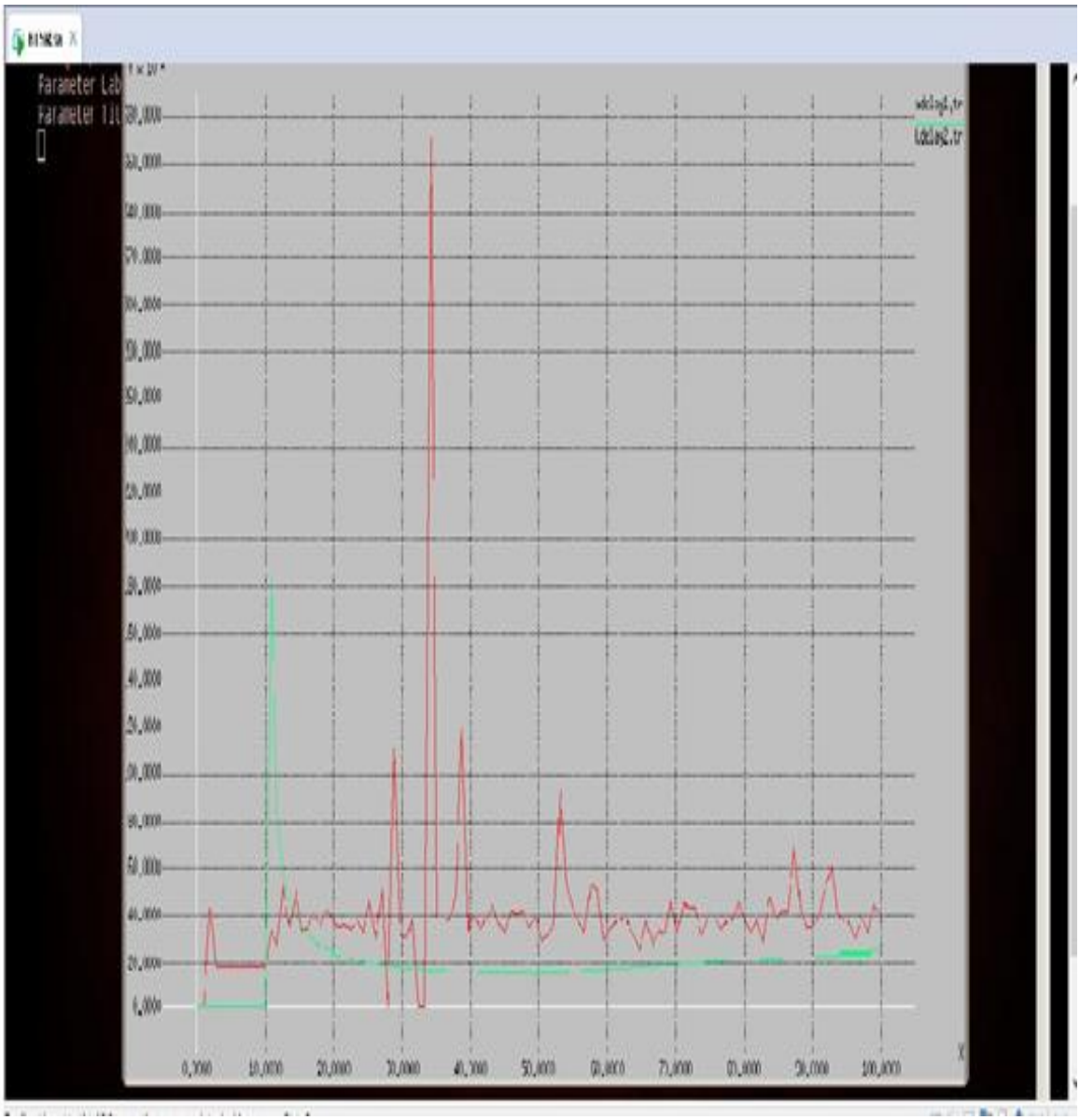


Figure 4.4 Delay graph between AODV and KAODV

B. According to the graph the kAODV algorithm delay rate (green) is better then the average dealy rate of aodv algorithm. Less delay mean less chance of intrusion.or more throughput..

4. 5 Output Graph.

#Xgraph alost.tr klost.tr

The output graph of this is as such.

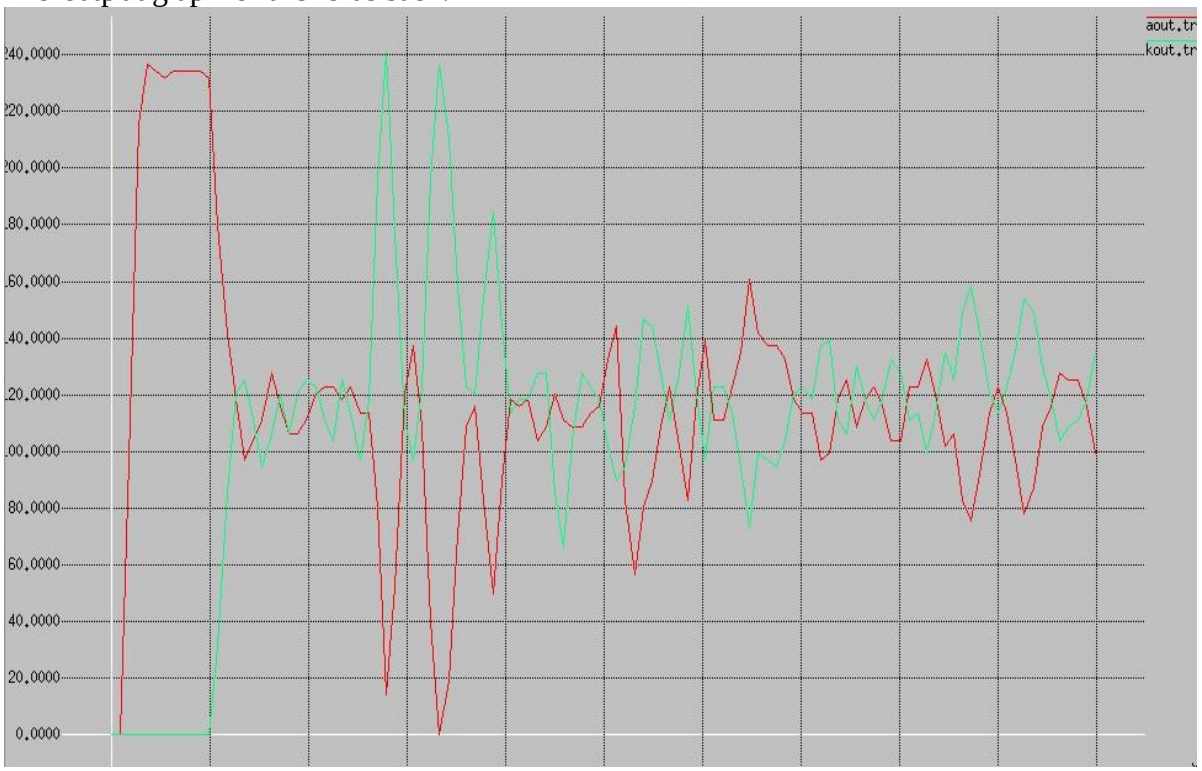


Figure 4.5 Output Graph

As per Graph showing the output of the KAODV is little bit better than the aodv and more consistent. The no of packet lost in the process of kodv transmission is lesser then the AODV. In the prospective of security this packet lost is almost negligible

Chapter 5

CONCLUSION AND FUTURE SCOPE

As this algorithm is, we can say an updated version of the AODV but which provide and load balancing or power of nodes. and this algorithm provide as the prevention mechanism also by not following any particular path by switch nodes for transmission because of the pdf factor change every time when every any packet go through an node .so the probability of a single node to transmit the data many time continually through it is very less .It provide us less hop count path also which is also improve the cost of the transmission. And dead node problem is also reduce. As we now in aodv protocol the algorithm send the packet through one node until the node don‟t come in dead state. So this algorithm provides us better power rate, less cost and reduce the probability of man in middle attack by frequently switching there nodes.

Future Scope: - There can be some feature work which we will do. Like we can use time parameter in the place of cost in the formula. if we can do work on their header packet by adding extra field in like power or use we can also improve path selecting formula.

Chapter 6

REFRENCES

I Research Papers

[1] ADRIAN PERRIG (2002), "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks", IJRSCT, p.125-130.

[2] Andreas Georgakopoulos, Kostas Tsagkaris, Vera Stavroulaki (2011), "Specification and assessment of a fitness function for the creation of opportunistic networks" Future Network & Mobile Summit 2011 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation, p.1034-1040.

[3] Chen xi, Tian youliang (2012), "Security in opportunistic networks" International Conference on Industrial Control and Electronics Engineering, vol.12, issue 4, p.456-450.

[4] C. E. Perkins and E. M. Royer, (2004), "The ad hoc on-demand distance vector protocol," in Ad hoc Networking, Addison-Wesley, pp. 173–219, 2000.

[5] (F.L.LEWIS)" To appear in Smart Environments: Technologies, Protocols and Applications. D.J. Cook and S.K. Das, John Wiley, New York, p.678-685

[6] Krishnamachar, (2005) Tutorial Presented at the Second International Conference on Intelligent. Sensing and Information Processing (ICISIP), Chennai, India,January.

[7] Luciana Pelusi, (2006), "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks", IEEE Communications Society, vol.44, issue 11, p.134-141.

[8] Suvadip Batabyal, Parama Bhaumik (2012) **"**Improving Network Performance with Affinity based Mobility Model in Opportunistic Network",IEEE Communications Society, vol.45, issue 12, p.234-241

[9] Swimpy Pahuja, A. Verma et al (2012) "An Effective Routing Scheme forSecure Data Dissemination over Sensor Networks", in Proc. of theAICTE Sponsored International Conference on Recent Trends in Computing Mechatronics and Communication (RTCMC 2012), p.789-795.

[10] Yixin Jiang, Chuang Lin (2006), "Mutual Authentication and Key Exchange Protocolsfor Roaming Services in Wireless Mobile Networks", IEEE Transaction on Wireless Communication, vol. 5, no. 9, p.2569-2577.

[11] Al-Sakib Khan Pathan (2010), "Security in Wireless Sensor Networks: Issues and Challenges", MIC and ITRC, p.1043.1047.

Chapter 7

APPENDIX

Glossary of Terms

- Model – It is a blue print of the or dummy of a big project in which we try different parameter on that dummy which is gona use in big project to see how it will work in that project.
- Trust – It is a type of promise or guaranty which give to the node that they will work under any condition.
- Ad hoc – Ad hoc is WN of structure which is not centralized. it does not depend on the environment by its nature of mobility .
- NS – its an network simulator which is use in to implement the network on the graphical way by creating its dummy.
- Node – An entities of the wsn which is connected to the network and communicate with other by using resource
- Trusted node – It is a node that provides the trust in the network that each message will be reached to their specified location and In case of any problematic scenario, it will be the responsibility of this node that will brings the network out from such situation.
- Mobility –It is the movement of the nodes which can move