ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Credit Risk and Self-Friendship tree Techniques for Greedy node Detection and Correction in Wireless Sensor Network using ns-2

Brahm Prakash Dahiya
A.P. in Computer Science Dept.,Shaym Lal College ,Delhi University, New Delhi, India.
brahmprakasd@gmail.com

***Abstract*—** In Wireless Sensor Network greedy node problem is very complicated. When the data transmission start and all node nodes make the connection with each other. During the data transmission some nodes are not cooperative for each other on recourse sharing, this types of node called greedy node. Many techniques are applied to detect the greedy nodes but they are failed to detect the greedy node. To avoid greedy node detection problem the author will propose a novel approach. In this paper the author will use credit risk technique to detect the greedy node and self friendship tree will use to correct the greedy node. In this paper the author will implement the greedy node detection and correction technique using the ns-2 simulator.

Keywords:- WSN, Greedy node, SFT, NS-2.

I. INTRODUCTION

Sensor networking is an emerging technology that has the ability to [1] monitor and manipulate the environment. The sensor network consists of a large number of sensor nodes that are densely deployed in the environment to monitor light, temperature, national security, health care, biological detection, etc. The base station collects data from all the nodes and analyzes the data to get the conclusion about the activity in that particular area. A sensor node has only finite energy supplied from a batter. It is often unfeasible to recharge the node's battery.

The energy consumption in a sensor node can be due to either "useful" or waste" resources. The useful energy consumption can be due to sending/receiving data, processing all the requests, sending the data to the neighboring nodes. Wasteful energy can be due to retransmitting data due to collision, idle listening, redundant nodes, wrong routing to send the data.

Communication between nodes consumes a lot of energy in sensor network. A centralized system also

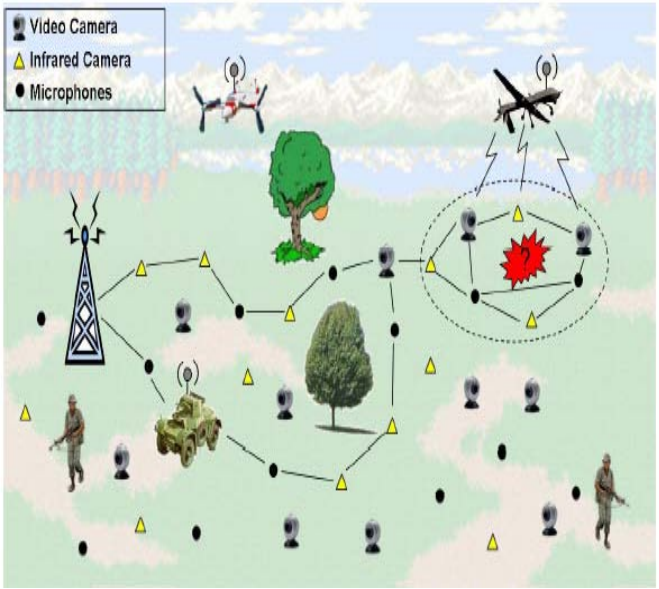

Figure. 1.1 Wireless Sensor Networ

Leads [3] to more energy depletion, as some of the sensor has to communicate a larger distance. Many routing techniques have been used to send the packets from a source to the destination.

II. LITERATURE SURVEY

In [1], the majority of existing detection approaches for WSNs focus on specific attacks, such as replication wormhole. Although they may indirectly detect compromised nodes, adversaries can avoid detection by avoiding the target attack

In [1] [2], the majority of the routing protocols can be classified into data centric, hierarchical, location based, network flow. Energy sensor node is assumed to know its own position as well as that of its neighbors which can be obtained with some localization schemes.

In [3] ,each node can forward packets to its neighbors within its transmission range that are closer to the sink node than itself. LEACH is a hierarchical routing algorithm for sensor networks. Nodes are bunched together into local cluster based on the signal strength. The cluster head of each cluster takes part in routing the data towards the sink. LEACH can't be applied to sensor networks that are deployed on a large scale since it assumes a single hop communication between a node and its cluster head.

In [4], the authors propose a Minimum Energy Gathering Algorithm (MEGA). The algorithm maintains coding tree and shortest path tree for delivering compressed data to the sink node.

Tubaishat et.al [5] proposes an energy efficient level based hierarchical routing protocols. Additionally it also provides secure routing protocol for sensor network [SRPSN] which provides protection against different kinds of attacks.

In [6], proposes an algorithm which will route data through a path whose nodes have the largest residual energy. The path is changed whenever a better path is discovered.

In [7], Directed Diffusion is a good candidate for robust multipath routing and delivery.

In [8] [9], a multipath extension of Dynamic Source

Routing (DSR) and Ad-hoc On Demand

Distance Vector (AODV) was proposed to improve the energy efficiency of ad-hoc networks by reducing the frequency of route discovery.

[10],The traditional method of detecting compromised nodes is to use attestation. Attestation is the checking of all or random portions of a node's memory for changes that would exist if the node was running altered code. The advantage of this approach is that it is capable to detecting compromised nodes that are not misbehaving. Several software-based attestation techniques have been proposed for WSNs. Unfortunately, secure software-based attestation has yet to be realized in WSNs and existing attestation techniques have been circumvented through various approaches, most of which have no hardware requirements beyond a laptop and serial cable.

[10], other approaches focus on monitoring communications for misbehavior. Misbehavior is decided using anomaly-based or rule-based approaches. Anomaly-based approaches establish a baseline behavior for neighbors and consider behavior that deviate from the baseline as anomalous.

III. PROBLEM FORMULATION

The author has found following problem based on the literature survey:-

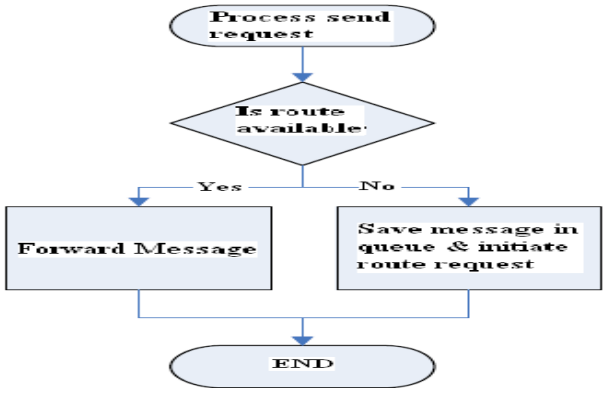

Figure 1.2 Existing System

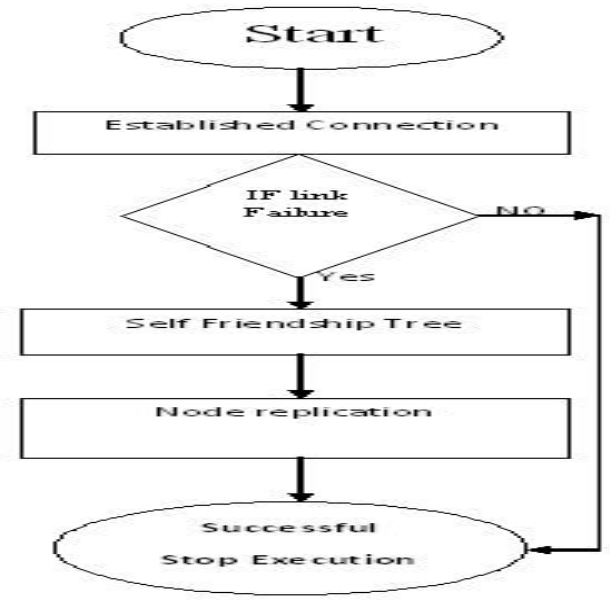

Figure 1.3 Proposed Systems

A. *Multipath Routing:*

The sensor nodes are distributed randomly in the sensing field. A network is composed of a sink node and many wireless sensor nodes. The sensor nodes have only limited power energy while the sink nodes have powerful resources to communicate with other nodes. The sensor nodes can be send or receive messages from other nodes. Each node has to select a particular and correct path to send the data. If the path is wrong, it may loss the data and loses its energy. As in [10], the path is selected based on the energy sufficient of nodes. The nodes with the more energy are selected to send the data packets. The destination node upon receiving the packet will reply with a route reply packet.

B. *Greedy node:*

These nodes aims to get the more benefit from the network like trying to preserve their energy or battery life or bandwidth. A greedy node may or may not send the data Packets in a proper way. A greedy node can do any of the possible actions in the network.

a. It may turn off its power when it does not have action communications with other nodes.
b. It may not forward all packets received from Any of its surrounding neighboring nodes to its correct neighboring destinations.
c. Sometimes the node sends some packets and drops others.
d. When a request is passed, it does not forward the reply request on reverse route.

Now the proposed algorithm will detect and solve the problem of Greedy node over wireless sensor network:

a) We develop a greedy node detection algorithm that considers partial greediness and novel replication allocation techniques to properly cope with greedy replication allocation.
b) The conducted simulations demonstrate the proposed approach outperforms traditional cooperative replication allocation techniques in terms of data accessibility, communication cost, and average query delay.

IV. IMPLEMENTATION OF EXISTING & PROPOSED WORK

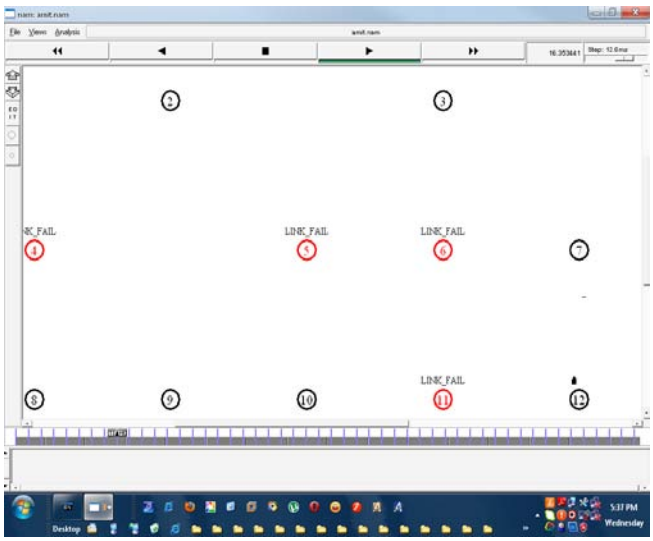

Figure 1.4 Implementation of Existing System

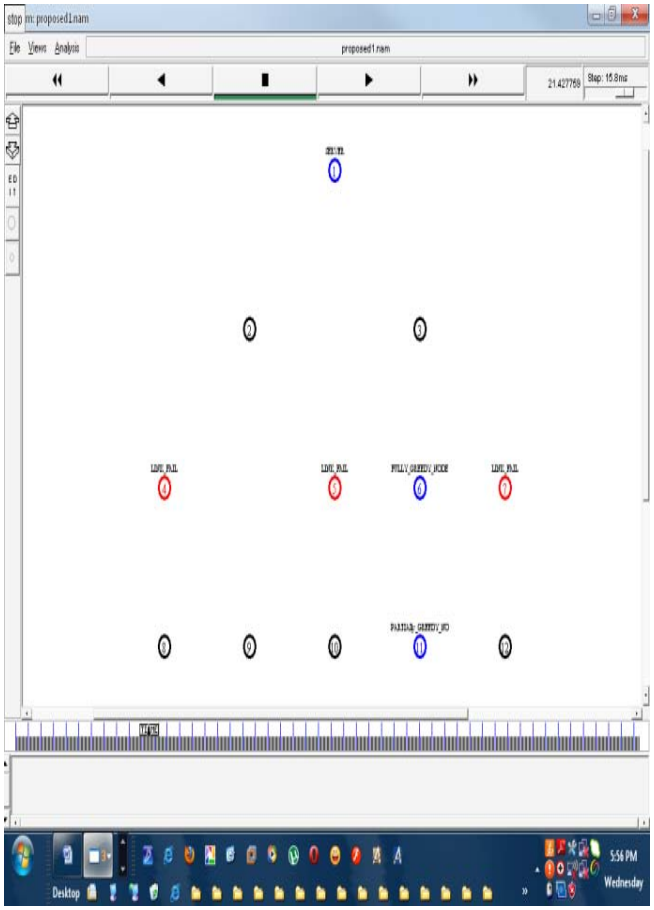

Figure 1.5 Implementation of Proposed System with Greedy node detection.

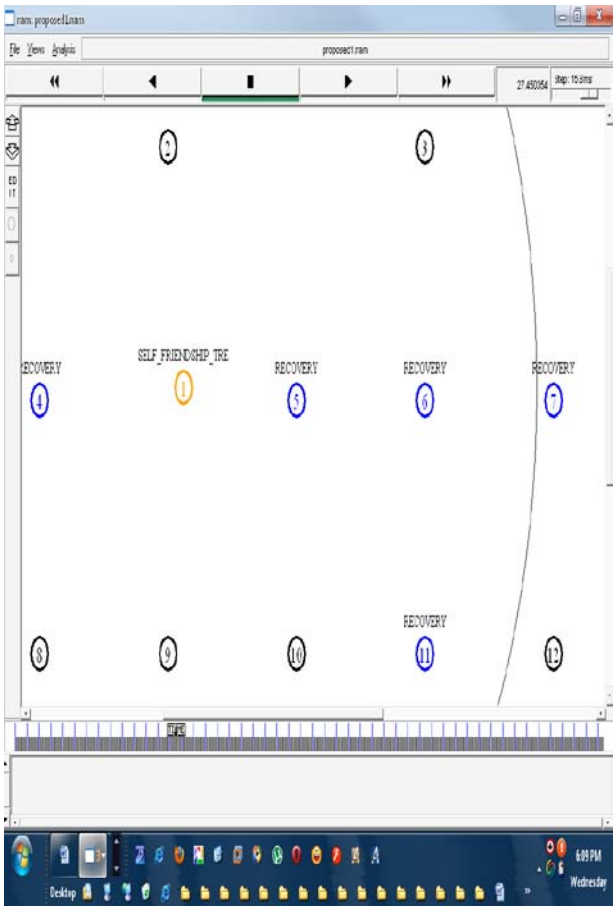

Figure 1.6 Implementation of Proposed System with Greedy node correction

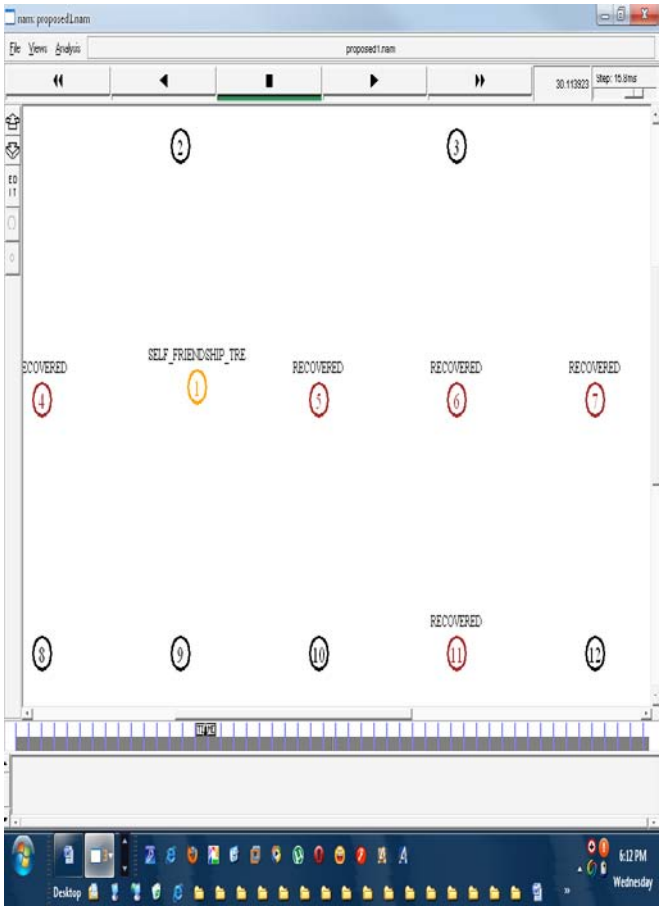

Figure 1.7 Implementation of Self Friendship tree

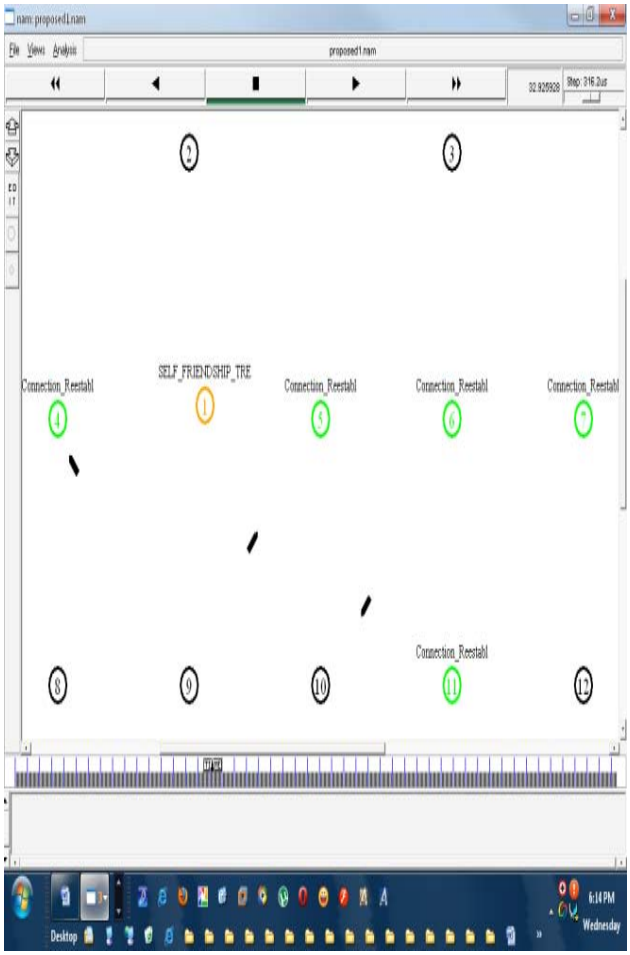

Figure 1.8 Connection re-establishment using proposed system

V. RESULT

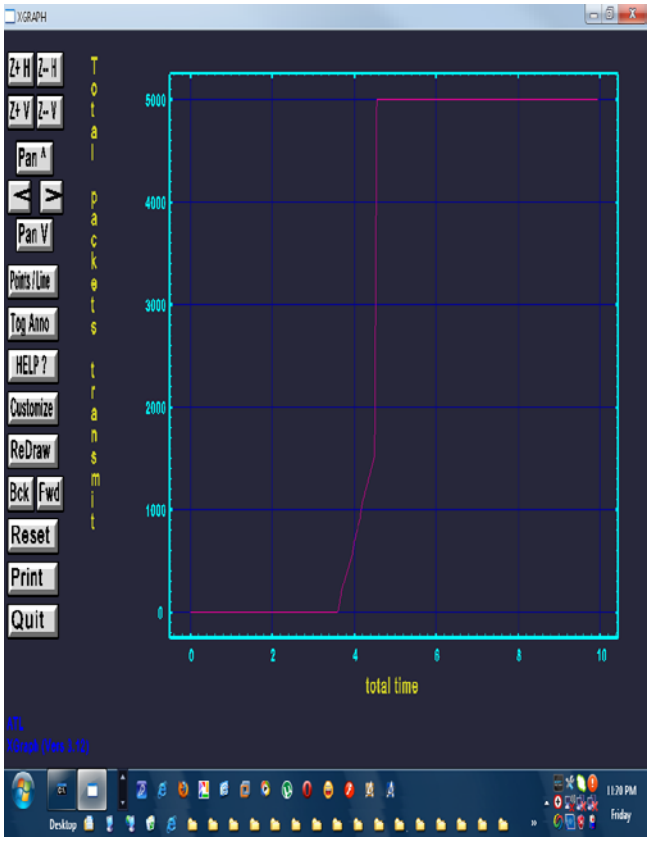

Figure 1.9 Total no of packets transmitted in exist system and proposed system

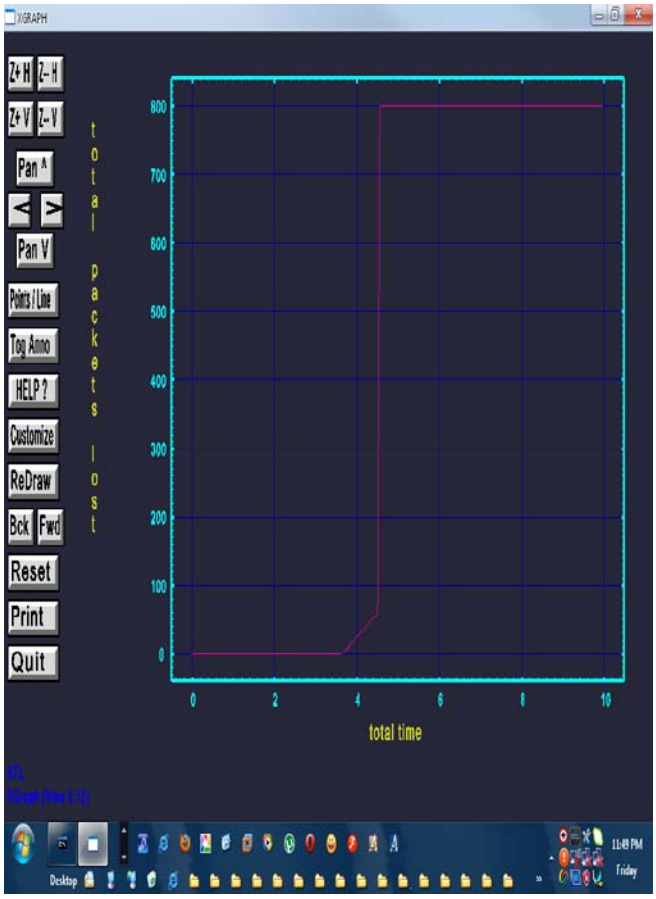

Figure 1.11 Total no of packets lost in exist system

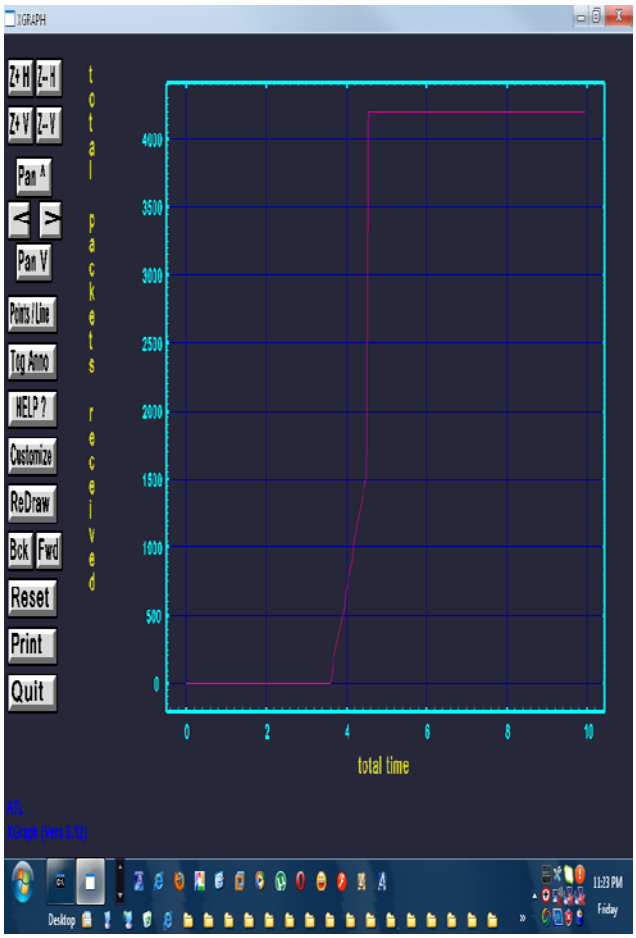

Figure 1.10 Total no of packets received in exist system

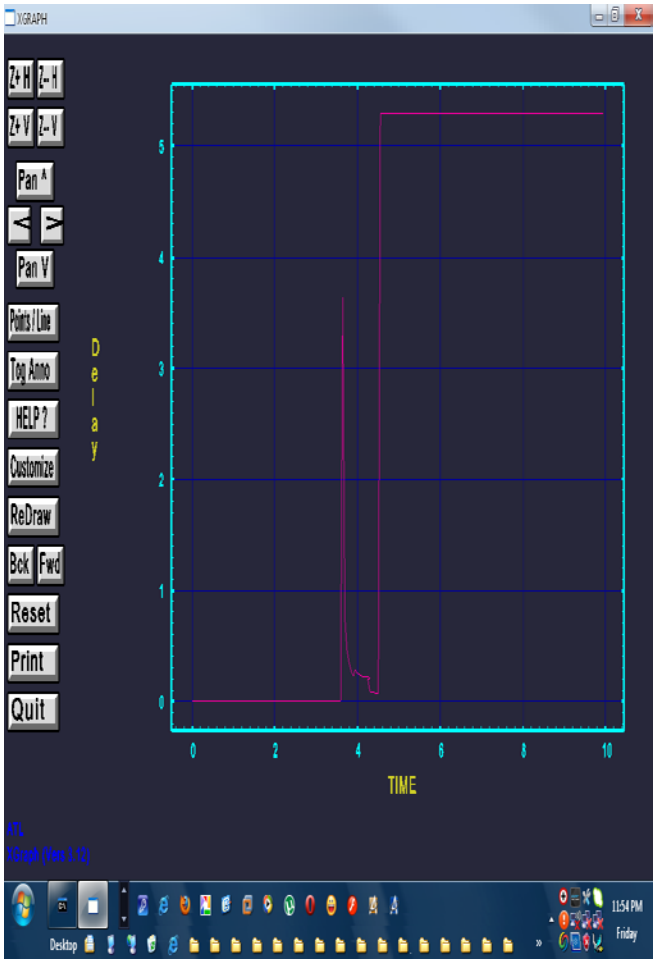

Figure 1.12 Delay in exist system

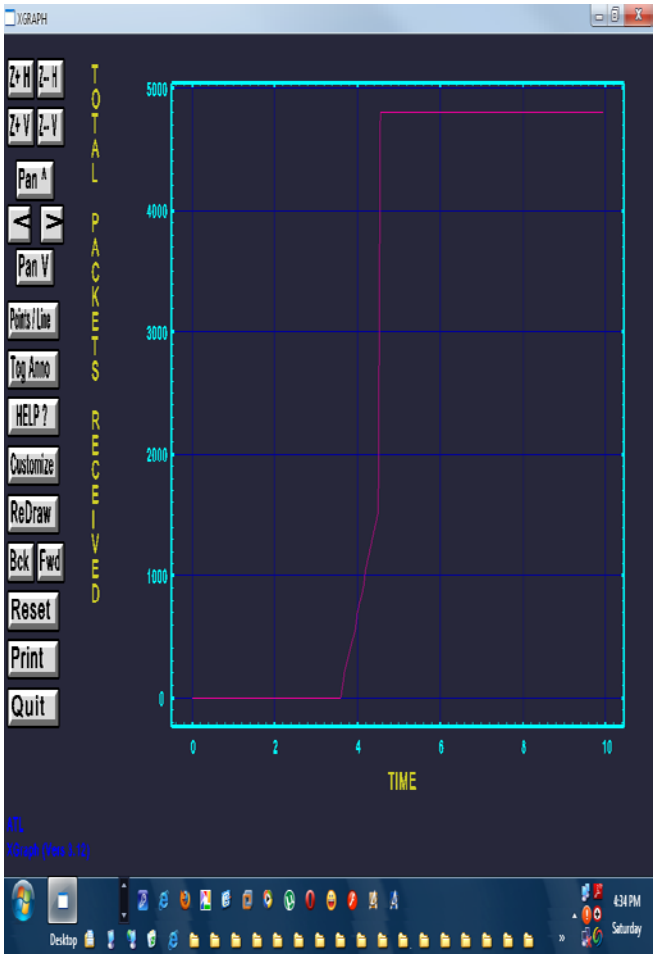

Figure 1.13 Total no of packets received in proposed system

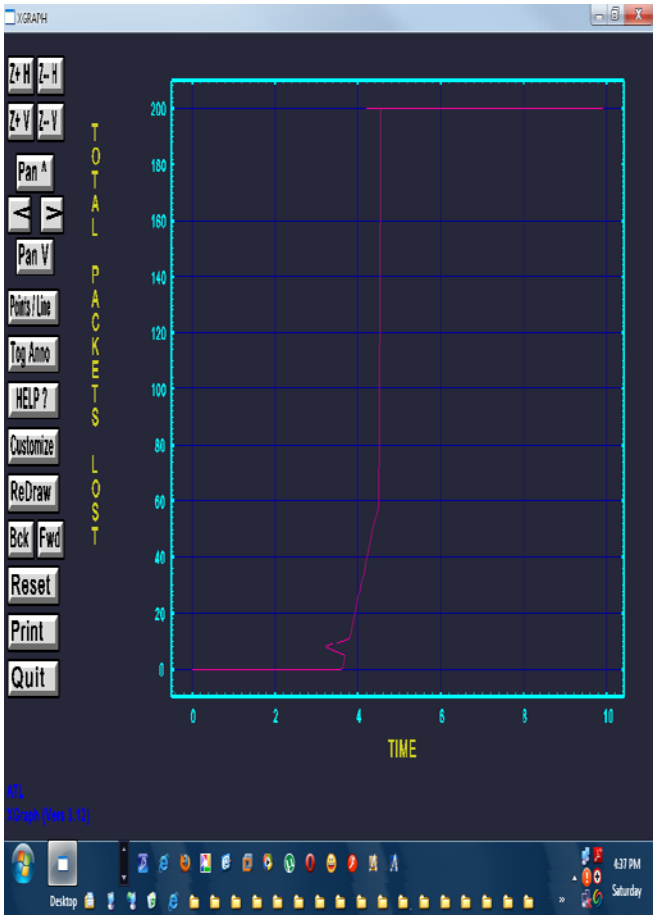

Figure 1.14 Total no of packets lost in proposed system

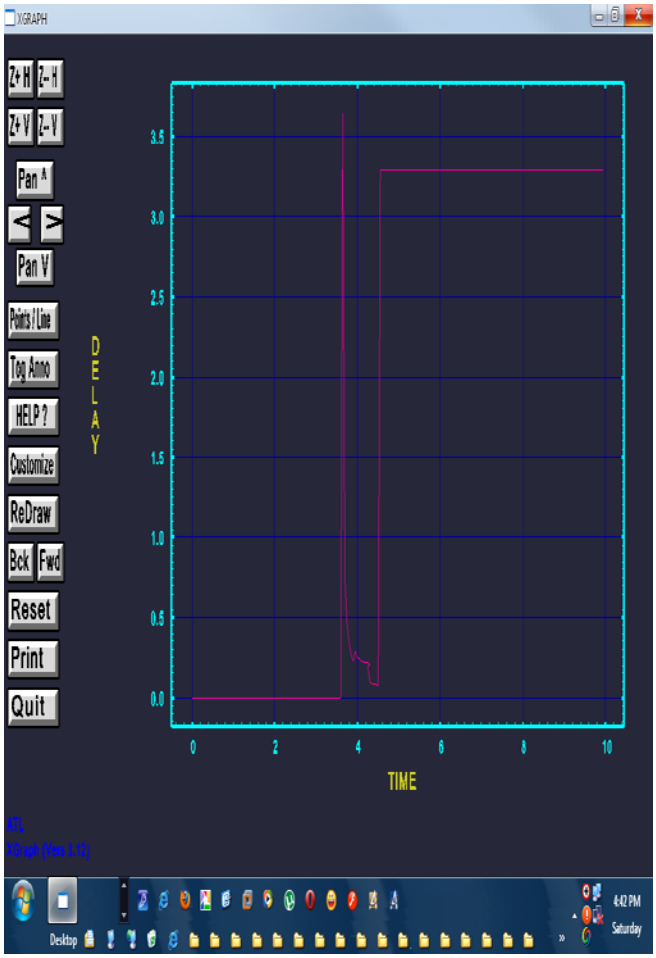

Figure 1.15 Delay in proposed system

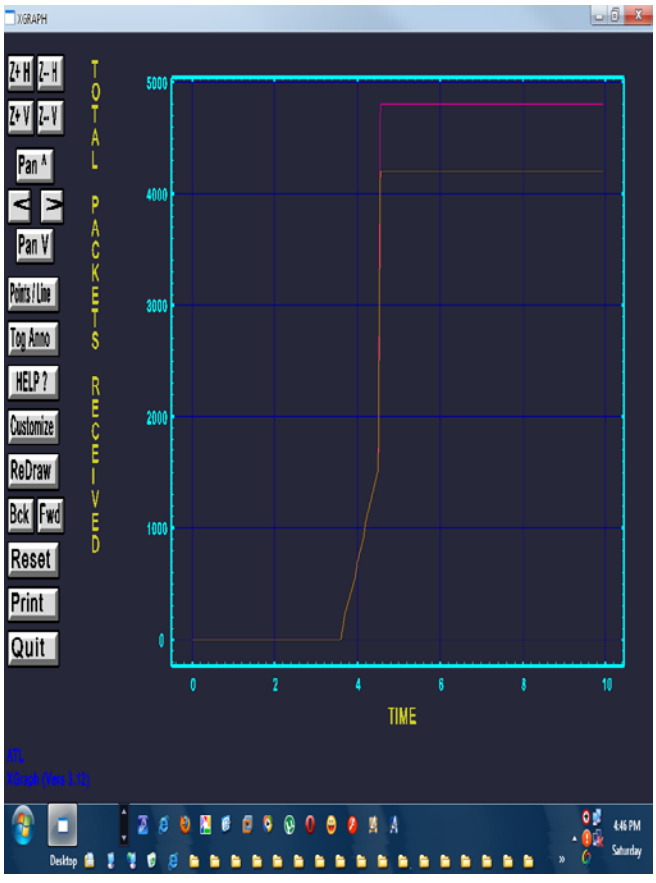

Figure 1.16 Total no of packets received in proposed system and existing system

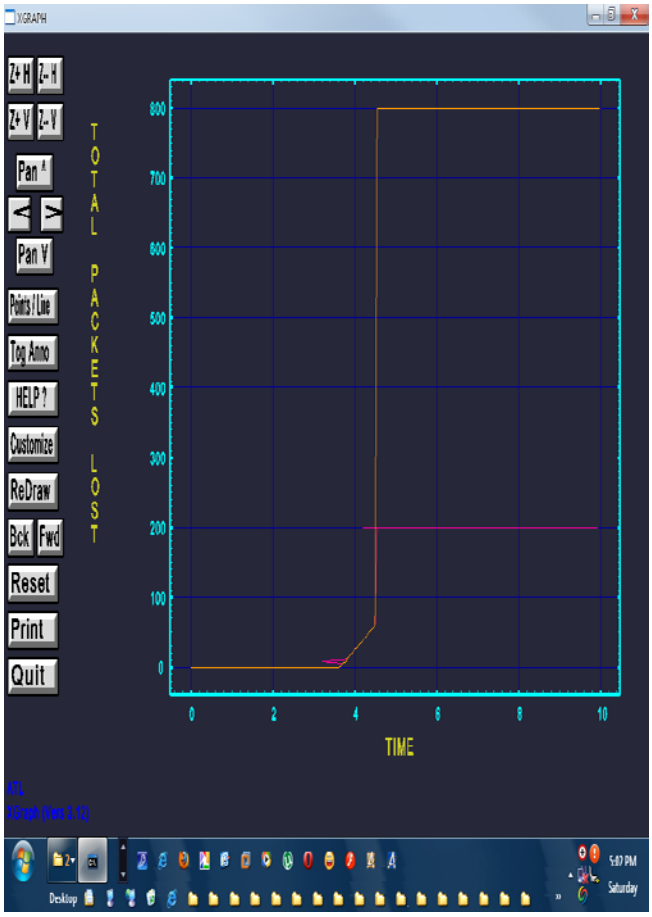

Figure 1.17 Total no of packets lost in proposed system and existing system

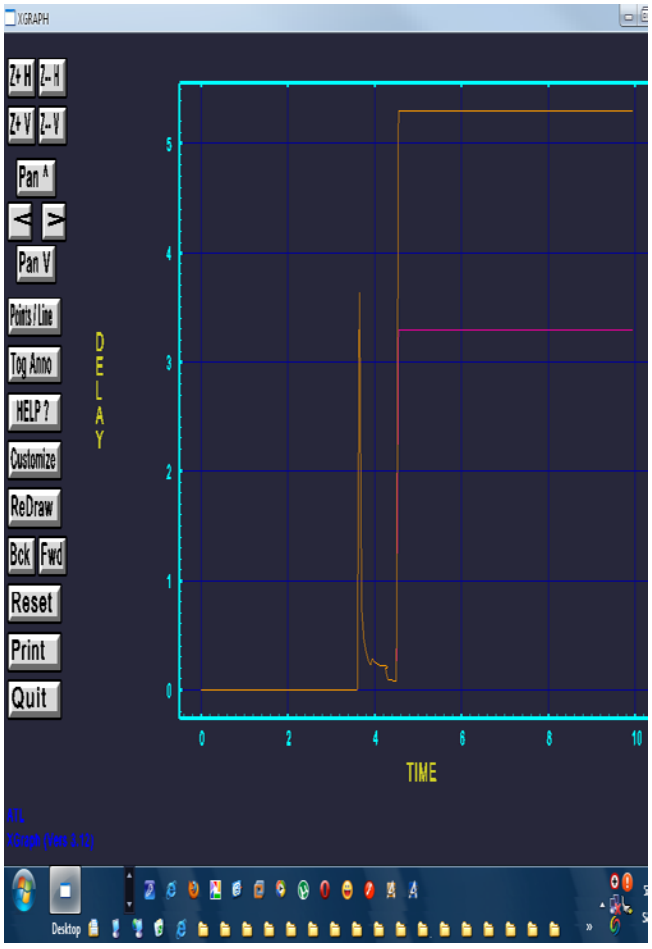

Figure 1.18 Total delays in proposed system and existing system

In the table 1 show comparison b/w existing system and proposed system bases on packets transmitted ,received, lost and delay .So the based on comparison the author proved the proposed system overcome the limitation of existing system using credit risk policy and self friendship tree to detect and correct the greedy node problem in wireless sensor network.

Table 1 Performance comparison between existing system and proposed system

Metrics	Existing System	Proposed System
Total packets transmitted	**5000**	**5000**
Total packets received	**4200**	**4800**
Total packets lost	**800**	**200**
Delay	**5ms**	**3ms**

VI. CONCLUSION AND FUTURE WORK

In this paper the author implemented the existing system and proposed system in Wireless Sensor Network with help of NS-2 simulator. The author overcome the limitation of existing system using credit risk policy and self friendship tree to detect and correct the greedy node problem in wireless sensor network. But using self friendship tree the storage wastage is increase. In the future work the author will utilize the storage or memory wastage problem in wireless sensor network.

VII. REFERENCE

[1] L.Doherty, L.El Ghaoni and K.S.J Pister, “Convex position estimation in wireless sensor networks” in Proc, IEEE INFOCOM April 2001, pp.1655-1663.

[2] Y.Shang, W.Ruml, Y.Zhang and M.P.J.Fromherz, “Localization from mere connectivity” in Proc MobilComm, June 2003, pp.201-212.

[3] Wendi Rabiner, Heinzelman and Anantha Chandrakaran and Hari BalaKrishnan, “Energy Efficient communication Protocol for Wireless Microwave network” In Proc, 33rd Hawaii International Conference on Mobile Computing, 2000.

[4] P.Von.Rickenbach and R.Wattenhofer, “Gathering correlated data in sensor networks” in Proc, DIALM.POML New York, 2004, pp 60-66.

[5] Malik Tubaishat, Jain Yin, Biswajist Panja and Sanjay Madria, “A Sensor Hierrarchical Model for sensor network” ACM SIGMOD Record 33, 2004, 7-13.

[6] J.Chang and L.Tassinlas, “Energy conserving routing in wireless ad hoc networks” in Proc of IEEE INFOCOM ’00, Tel-Aviv, Israel, March 2000, pp-22-31.

[7] S.Tilak, N.b. Abu-ghazaleh and W.Heinzelman, “A Taxonomy of Wireless micro sensor network models”, Mobile computing and Communications Review, Vol 6, No.2, pp.28-36, 2002.

[8] A. Naripuri and S.Das, “On Demand multipath routing for ad-hoc networks”, in Proc of International Conference on Computer Communications and networks”, Boston, UA, USA, Oct, 1999.

[9] M.Marina and S.Das, “On Demand multipath distance

vector routing in ad-hoc networks" in Proc of the ninth International Conference for network protocols(ICNP), Riverside, Ca, USA, Nov 2001.

[10] R.VidhyaPriya, Dr. P.T.Vanathi, "Energy Efficient Adaptive Multipath Routing for wireless sensor networks", International journal of computer science, 2007.