Quad Cluster: A Promising Approach For Black Hole Prevention In Manet

Ms. Veena K Lalbeg[1], Mr. S.S.Sannakki[2], Mr. Sanjay Chakalabbi[3]
P.G Student[1], Professor[2], Developer[3]
Department of Computer Science and Engineering
1,2Gogte Institute of Technology, Belagavi (Karnataka), India, 3Unisys Global Services, Bangalore
1veena.lalbeg@gmail.com,2sannakkisanjeev@git.edu,3sanjay.chakalabbi@gmail.com

Abstract: This system adheres to the security and performance issues of MANET. The proposed system inhabits the concept of quadrant based clustering which successfully reduces the overhead and flooding and leads to cluster head to cluster head communication. Also adds a strong Intrusion Detection System which uniquely validates and verifies every node being deployed in the mobile ad hoc network, due to which the detection and prevention of a black hole attack, is accomplished before its successful penetration into the network. Hence the proposed system produces results with increased packet delivery ratio, throughput and decreased end to end delay and proves to be a better system overall.

Keywords: Black hole attack, MANETs, Security, Cluster, Malicious node, Data Packets, Throughput, IDS

I. INTRODUCTION

Highlight a section Mobile ad hoc network is an autonomous system of mobile nodes, connected by wireless links without existence of any infrastructure hence the name infrastructure less, in MANET .MANET comes across many challenges such as: lack of infrastructure, power consumption, existence of dynamic topology, and security threats. Security threats in MANET presents a larger security challenge if it is compared to conventional wired and wireless networks, mainly due to the common vulnerabilities of wireless connection, one of the most famous security threats in MANET is black hole attack[1]. There are many researches proposed and implemented to address this security issue, some researches succeed in preventing this attack considerably but not completely, the point of comparison or differentiation between these solutions is not only the success degree of the detection, but also is how much these solutions may not affect the performance of the network. MANET nodes might have very limited resources, making it difficult to tackle rigid attacks. Various types of attacks have been identified and depending upon the category of attack , solutions are proposed and implemented with a scope to devise better results which making this area of research more interesting.

II. PROBLEM DEFINITION

Mobile Ad-hoc Networks with respect to their natural behavior and characteristics are more susceptible to threats. One among the severe threats is the black hole attack which advertises fake routes during the path discovery process and drop, duplicate or spoof the data packets once the route advertised by it is selected causing the network to fail. Hence the proposed system tends to detect and prevent the black hole attack using a strong intrusion detection system along with clustering technique which tends to improvise the overall network performance and also increase the throughput and packet delivery ratio of the system.

III. BACKGROUND THEORY

A. Intrusion Detection System based on Mobile Agents

The authors in this approach [1] propose a new Intrusion Detection System (IDS) based on Mobile Agents. Mobile Agents (MA) are used that can move from one node to another node within a network. The computation complexity caused by using MA is kept to minimum level so that overhead involved can be reduced. This scheme raises the efficiency of every node thereby increasing the overall performance of the network. Besides, the system also tends to decrease the computation overhead in each node in the network.

B. Reputation Based scheme

In a reputation based scheme [2] watchdog and path rater approach is introduced as the IDS to listen in the nearby nodes packet transmission promiscuously and indicate misconduct of any spiteful node to the source node by sending a message. The source node on collecting the information checks every node to avoid untrustworthy nodes in discovering a path. CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad-hoc Networks) [2], here the IDS utilizes a distributive approach to monitor node promiscuously, observes the route protocol action and transmission of neighboring node packets. On detection of any inappropriate action the trust manager sends an ALARM message. Rating list and black list for malicious nodes is maintained by the reputation system. A rank is maintained for each node according to the reputation they hold by the path manager. The IDS here is not strong enough as it depends on other nodes which reduce the reliability of the system.

C. Watchdog Solution

Marti et al. [3] proposed an innovative scheme to improve the performance of the network by increasing its throughput in the presence of a spiteful node and named the approach as

.

Watchdog. This scheme is actually divided into two parts, the basic Watchdog and Pathrater. Watchdog working as an intrusion detection system is responsible for detection of the indecent node in the network. Watchdog node maintains a failure counter for node that fails to forward the packet ahead within a given time. If the failure counter of any node crosses its threshold the Watchdog node declares that node as misbehaving. Pathrater [4] here in connection with the routing protocols reject any such transmissions that are been generated from the reported nodes.

IV. ROPOSED SYSTEM

B. SYSTEM ARCHITECTURE

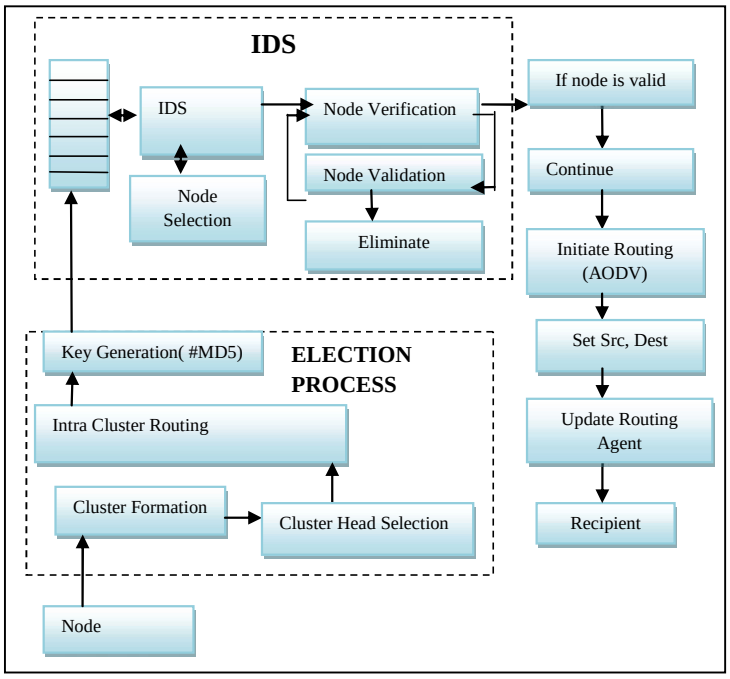

Fig 1: System Architecture

B. WORKING PROCESS OF THE SYSTEM

With respect to the system design shown in fig 1 explained as follows:

1. Node Deployment

Nodes are created and deployed randomly into the network.

2. Election Process

Once nodes are deployed into the network, region or quadrant separation of the network is initiated. Every region receives a certain number of nodes along with the initial energy .Once these regions are established, the proposed system looks for neighboring nodes in the network, which is found using the minimum distance of the nodes.

3. Cluster Formation and Cluster Head Selection

Under cluster formation, clusters are formed using the Received signal strength indicator. Every cluster has a cluster head, which is selected using the cluster head selection process. Once CH selection process is over inter cluster routing process takes place.

4. Key Generation

The proposed system makes use of the popular MD5pure algorithm for generation of unique keys. These keys are given to each and every node during the node creation and deployment process. Later the intrusion detection system uses these keys to involve only valid nodes with unique key to process routing in MANET.

5. Intrusion Detection System(IDS)

IDS act as the backbone of the proposed system. It is initiated (or called) when the nodes are deployed in the network. IDS plays very important and crucial role in node selection as it initiates the authentication process by verifying and validating every node in the network. If the nodes are valid they remain in the network and accomplish the routing process successfully. If the node is not valid then such a node is detected and eliminated from the network. This is how the IDS prevent the black hole attack from penetrating into the network.

6. Routing Process

Once the IDS eliminate the attacker, routing process is initiated with the rest of valid nodes. The routing protocol used here is the AODV protocol. With stable or shortest path established the routing process is accomplished with minimum delay, packet loss and higher packet delivery ratio.

V. IMPLEMENTION

A. Region Division-Quadrant based

Here the simulation area is divided into four regions or quadrants. Considering the x coordinate and y coordinate values of the nodes provided in the topology file, the nodes are distributed to each region in the network. So every region will hold a certain number of nodes. The flowchart 2 corresponds to the above mentioned process.

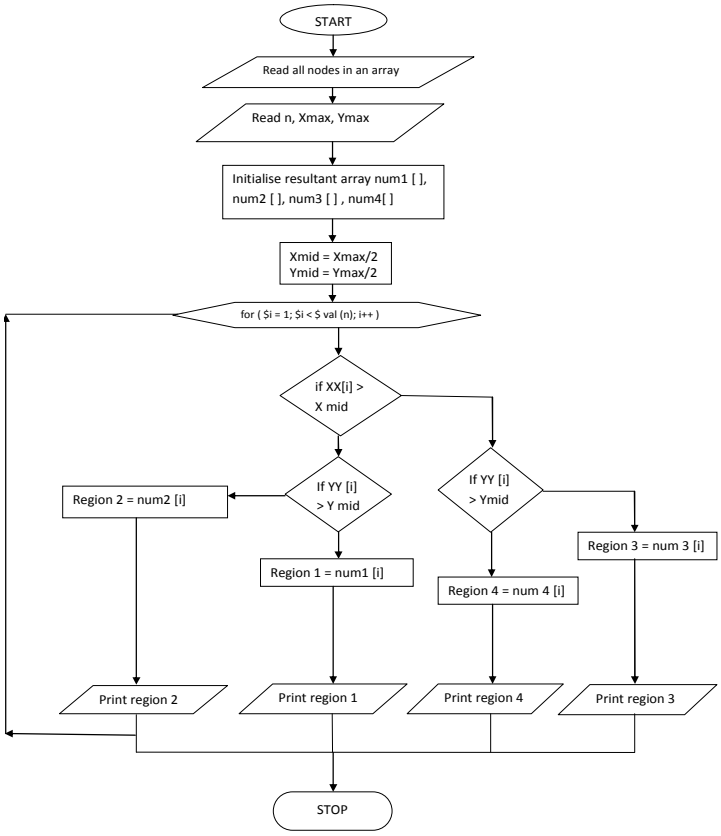

Fig 2: Region Division Quadrant Based

B. Cluster Header Selection

In this step cluster head is selected through the selection process shown in fig 3.

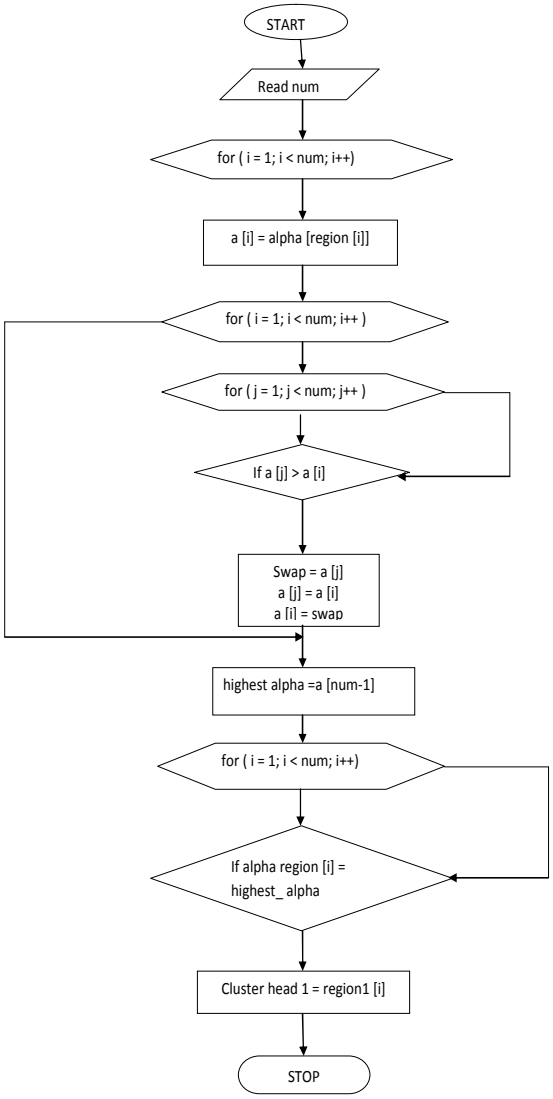

Fig 3:Cluster Head Selection

VI. RESULT ANALYSIS

A. SIMULATION

The proposed system is implemented using the network simulator NS2 in Linux open source environment with the following parameter set (Table 1) .

Table 1: Simulation parameters

Parameters	Values
Channel	Wireless Channel
Propagation	TwoRayGround
Network Interface	Wireless Physical
Mac Type	802_11
Max Packet Queue Length	500
Number of Nodes	50
Area	450X450
Routing Protocol	AODV
Link Layer	LL

.

B. EVALUATION

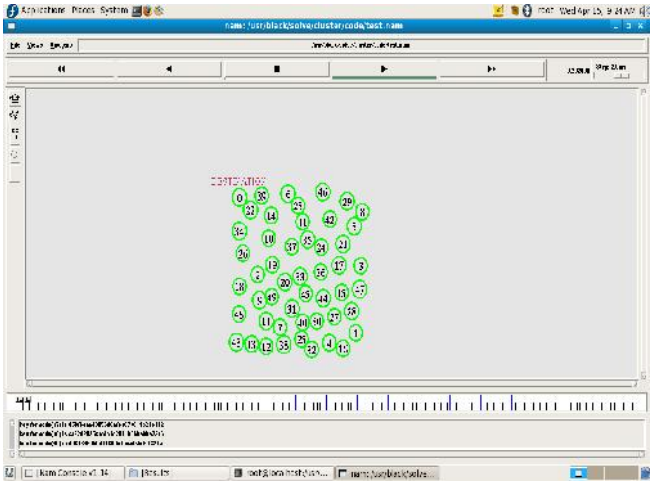

Fig 4: Node deployment

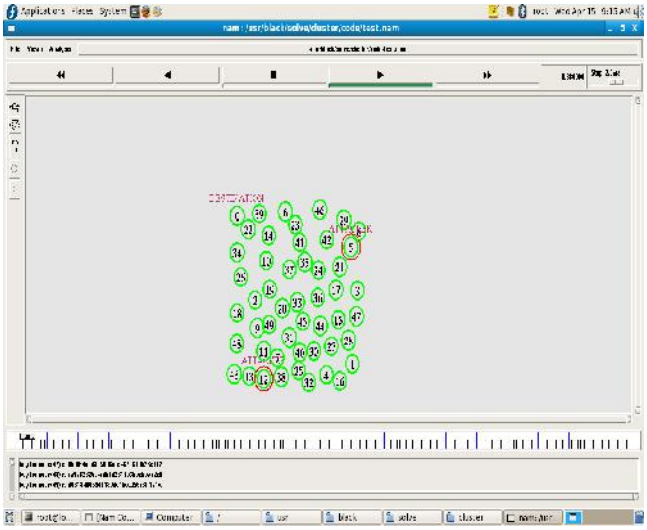

Fig 5: Attackers identified

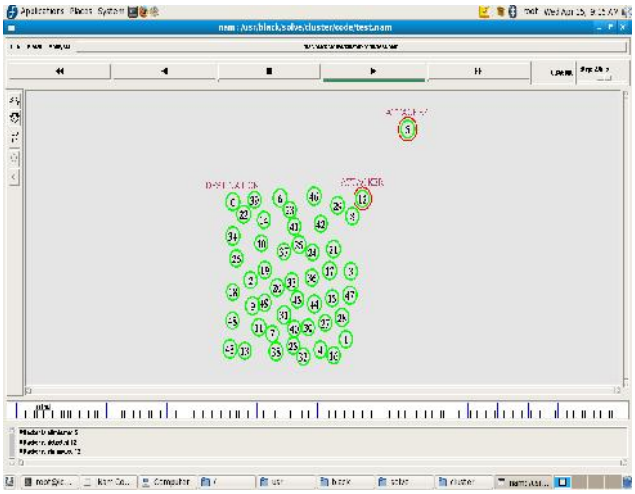

Fig 6: Attackers are eliminated

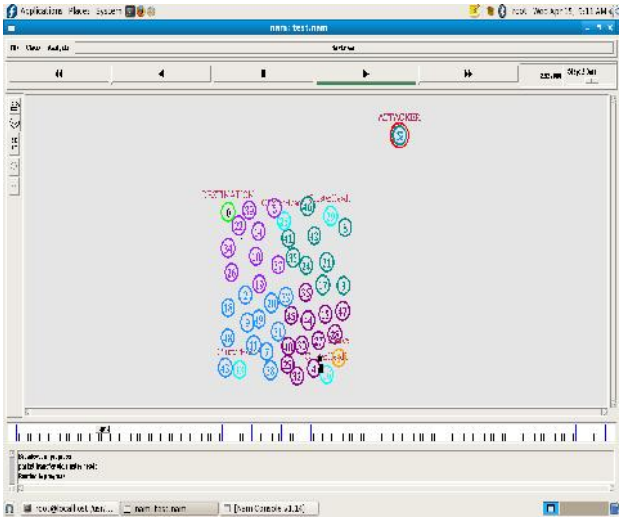

Fig 7: Cluster Formation

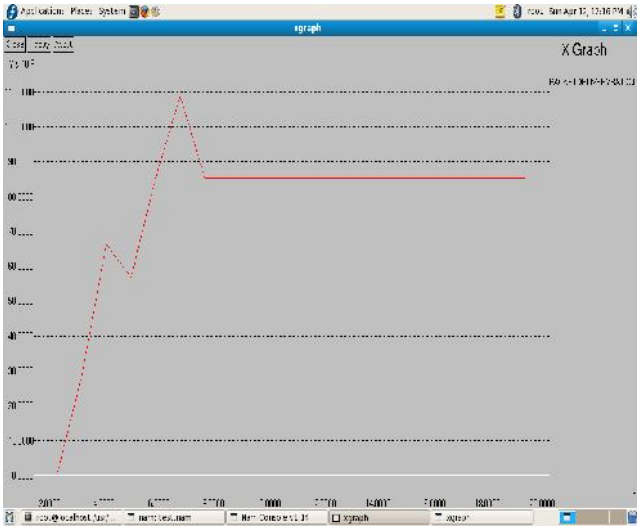

Fig 8:Increased Packet delivery ratio

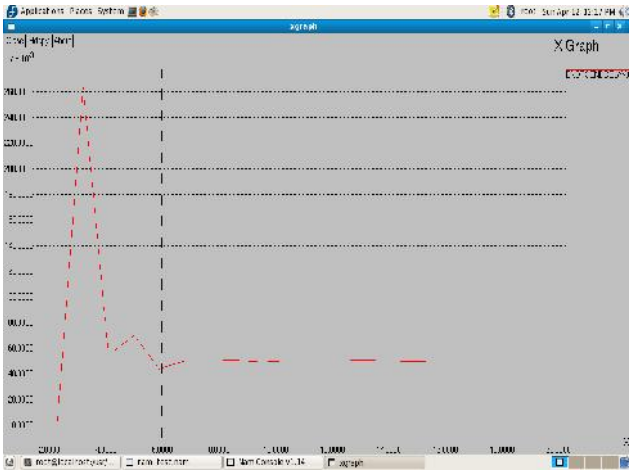

Fig 9: End to End delay

.

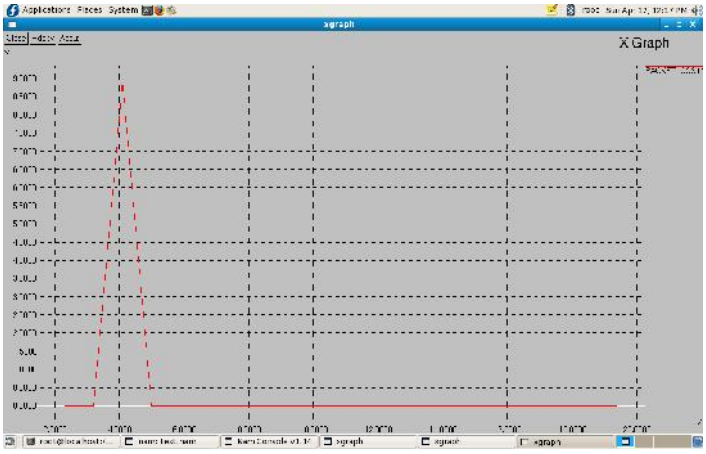

Fig 10: Decreased Packet loss

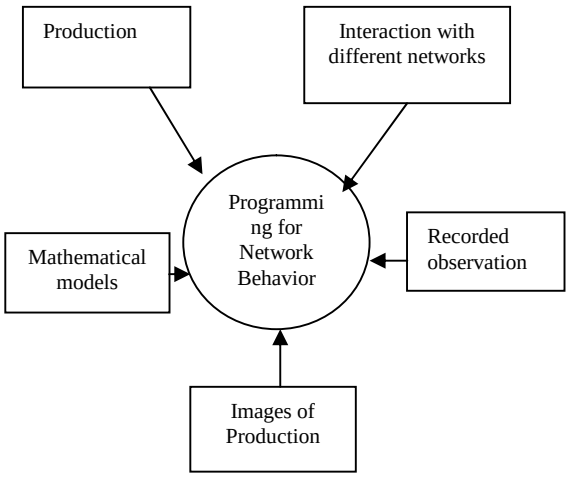

Figure A.4.1: Basic requirements of network behavior.

VII. CONCLUSION

The proposed system inhabits the concept of quadrant based clustering which successfully reduces the overhead and flooding and lets cluster head to cluster head communication. Also adds a strong Intrusion Detection System which uniquely identifies every node being deployed in the network due to which the detection and prevention of a black hole attack before penetration into the network is accomplished. Hence the proposed system produces results with increased packet delivery ratio, throughput and decreased end to end delay.

VIII.

IX. FUTURE WORK

With respect to the system implemented, future work of the system would be to use a fully dynamic topology to address complex network plus develop a strong encryption and decryption process for the packets being transmitted from one source to destination. Also to explore attacks like worm hole and grey hole and implement the further process in NS3 Network Simulator.

APPENDIX

SOFTWARE DESCRIPTION

Network simulation is a technique in which network behavior is modeled using program. Program does this by computing the communication between the different network entities (hosts/routers, data links, packets, etc) using mathematical formulas, taking and playing back recorded observations from a production network. Further, the behavioral study of the network with its various applications and services can be observed in test lab. During testing, modifications to the various attributes of environment can be controlled to assess behavior of the network. Sometimes to observe end-to-end performance, simulation is used with conjunction with live applications and services; this technique is referred as network emulation.

Motivation for Simulation(s):

Simulation have become one of the most acceptable and research tool in system analysis and research because of its key features such as; computing abilities at less time, various methodologies, use of various languages etc. Following can be considered as motivational factors for simulation

1. It does not require special purpose equipment or can be managed by internally available resources; hence it does not cost much.
2. It enables study of complex scenarios with, the interaction of internal complex situations.
3. It simulates new design before implementation hence results can be used for forecasting of any situations.
4. Changes in design can be easily altered in less time; hence it reduces total process time.
5. Animation of any system can be used for better visualization

Advantages of simulation:

Simulation mimics the real system or it visualizes system in design stage. These days simulation models are developed for solvable mathematical models. It is because of these few reasons simulation is a natural choice for problem solving. Following are few advantages of simulation.

1. In normal analytical techniques, assumptions are made to develop mathematical model which invites for restrictions on the model. At the end which results in flawed output. Simulations avoid placing unnecessary restrictions on the model and it considers random process into account.
2. Analysts can visualize relationship between various components of the system in detail before implementation. In other words, it helps to explore without disturbing ongoing operations of the working environment.
3. Additionally, as stated above it allows comparing different systems which helps to decide optimal system.
4. Insight about importance of variables into operating systems gives us knowledge which can be used at later stages.
5. It enables feasible study for various hypothetical questions. (How? why? what?)

Disadvantages of simulation:

1. Simulation is an art which is mastered over a time, which requires special training, special resources which comes over experience.
2. In some situations it is difficult to develop model, difficult to interpret results which may lead to further complications.
3. The results are the only estimates or projected outcomes.
4. Sometimes modeling leads for consumption of time which ultimately costs the available resources.
5. Simulation models are optimized for given model character and a set of input which are based on limited number of variables.

REFERENCES

[1] Debdutta Barman Roy and Rituparna Chaki, "MADSN: Mobile Agent Based Detection of Selfish Node in MANET "International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.

[2] A.S. Anand, M. Chawla, Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010.

[3] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," 6th MobiCom, Boston, Massachusetts, August 2000.

[4] Mohammad Mubasheer et al, EAACK—A Secure Intrusion-Detection System for MANETs International Journal of Computer Science and Mobile Computing, Vol.3 Issue.10, October- 2014, pg. 969-975.

About Authors:

1. **Ms.Veena K. Lalbeg, BE, MTECH in computer science & engg, GIT, College Belagavi, Karnataka. Published paper on Clustering Of Mobile Ad Hoc Networks, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 2, Special Issue (NCRTIT 2015), January 2015. ISSN 2348 – 4853**

2. **Prof. S.S.Sannakki, Department of computer science and engg, GIT, College, Belagavi, Karnataka.**

3. **Mr. Sanjay Chakalabbi, BE in computer science & engg, SGBIT, Belagavi, Karnataka. Developer at Unisys Global Services, Bangalore Karnataka.**

.