A Cluster Based Walk for Peer To Peer Streaming In Wireless Sensor Networks

J. Sebastina Queen Rose, S. Sumithra

***Abstract*---- In the performance evaluation of a protocol for an ad hoc network, the protocol should be tested under realistic conditions including, but not limited to, a sensible transmission range, limited buffer space for the storage of messages, representative data traffic models, and realistic movements of the mobile users (i.e., a mobility model). Simulation is universally considered the most effective method of designing and evaluating new network protocols. When developing protocols for mobile networking, the chosen mobility model is one of the key determinants in the success of an accurate simulation. The main role of a mobility model is to mimic the movement behaviors of actual users. Given the critical role of the mobility model in supporting realistic and accurate protocol simulations, its correct design and selection is essential .We have described 3 mobility models that represent mobile nodes whose movements are independent of each other (i.e., entity mobility models). If the number of data is less than the number of cluster then we assign each data as the centroid of the cluster. Each centroid will have a cluster number. If the number of data is bigger than the number of cluster, for each data, we calculate the distance to all centroid and get the minimum distance. This data is said belong to the cluster that has minimum distance from this data. Since we are not sure about the location of the centroid, we need to adjust the centroid location based on the current updated data. Then we assign all the data to this new centroid. This process is repeated until no data is moving to another cluster anymore. Mathematically this loop can be proved convergent .**

Key Words: Mobility model, centroid, cluster.

1. INTRODUCTION

Peer-to-peer (P2P) content sharing technologies like Napster, Gnutella, and Kazaa are applications that have been astonishingly successful on the Internet. P2P has gained tremendous public attention through Napster which is a system supporting music sharing on the Web. It is an emerging and interesting research technology with a promising product base. Intel P2P working group gave the definition of P2P as "The sharing of computer resources and services by direct exchange between systems". This thus gives P2P systems two main key characteristics: Scalability and Reliability. In Scalability, there is no algorithmic, or technical limitation of the size of the system, e.g. the complexity of the system should be somewhat constant regardless of number of nodes in the system**.** In Reliability, the malfunction on any given node will not affect the whole system (or maybe even any other nodes). File sharing networks like Gnutella is a good example of scalability and reliability. In Gnutella, peers are first connected to a flat overlay network, in which every peer is equal. Peers are connected directly without the need of a master server's arrangement and the mal function of any node does not cause any other nodes in the system to malfunction as well. P2P can be categorized into two groups classified by the type of model: pure P2P and hybrid P2P. Pure P2P model, such as Gnutella and Free net, does not have a central server. Hybrid P2P models, such as Napster, Groove and Magi, employs a central server to obtain meta-information such as the identity of the peer on which the information is stored or to verify security credentials. In a hybrid model, peers always contact a central server before they directly contact other peers.

The main role of a mobility model is to mimic the movement behaviors of actual users. Given the critical role of the mobility model in supporting realistic and accurate protocol simulations, its correct design and selection is essential .We have described 3 mobility models that represent mobile nodes whose movements are independent of each other (i.e., entity mobility models). If the number of data is less than the number of cluster then we assign each data as the centroid of the cluster. Each centroid will have a cluster number. If the number of data is bigger than the number of cluster, for each data, we calculate the distance to all centroid and get the minimum distance. This data is said belong to the cluster that has minimum distance from this data. Since we are not sure about the location of the centroid, we need to adjust the centroid location based on the current updated data. Then we assign all the data to this new centroid. This process is repeated until no data is moving to another cluster anymore. Mathematically this loop can be proved convergent.

In this paper, we proposed a Network Coding (NC) based on rateless codes, that are being based on simple AND operations are computationally efficient. We also propose the Clustering technique. It is an algorithm to classify or to group the objects based on attributes/features into K number of group. K is positive integer number. The grouping is done by minimizing the sum of squares of distances between data and the corresponding cluster centroid. Thus, the purpose of K-mean clustering is to classify the data. The cluster head has selected based on residual energy and throughput. We are going to clustering for security and providing good QOS.

2. BLOCK DIAGRAM

The basic block diagram is shown in fig 1. The main aim of the system is to avoid energy wastage and collision by using Clustering technique. The work station consists of multiple nodes. First of all the nodes are created and initialized. Then it is used to form the cluster. Each cluster group contains one cluster head and number of cluster

ISSN: 2278 – 7798

member. The cluster selects the channel based on MR HEED algorithm. And then goes to base station and analyze the performance.

These below blocks perform the main function of the system.

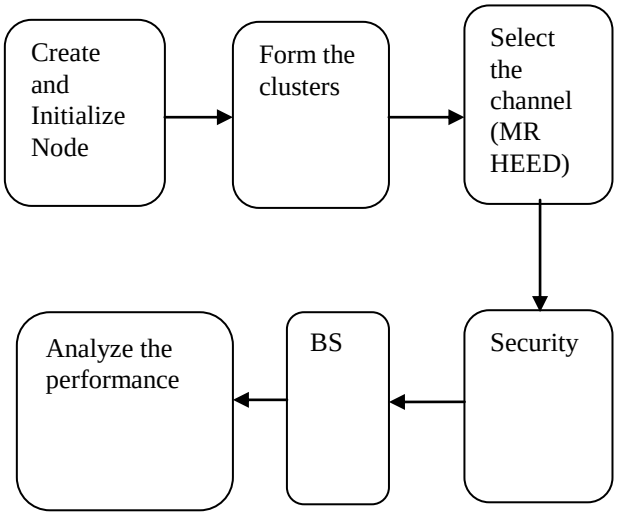


Fig.1. Block diagram

Security algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption. A public key, which may be known by anybody, and can be used to encrypt messages. A private key, known only by the recipient, and used to decrypt messages. Also we are using AND operations for security. The fig 2 shows analysis of cluster formation in step by step. First the nodes are deployed and select the anchor node. The node sends route request(RREQ) message to the cluster head. The cluster head is the high energy node. The cluster head is selected using two parameters. These parameters are residual energy and throughput. Using hierarchical routing protocol, the cluster head has been formed. This hierarchical routing protocol consumes low energy and used to avoid the energy wastage. It sends route reply(RRPY) message to the required node. The Artificial Bee Colony algorithm is used to select the path. The node starts to send the packet. If the number of data is bigger than the number of cluster, for each data, we calculate the distance to all centroid and get the minimum distance. This data is said belong to the cluster that has minimum distance from this data. Since we are not sure about the location of the centroid. Then we assign all the data to this new centroid. This process is repeated until no data is moving to the another cluster anymore and then provide better performance.

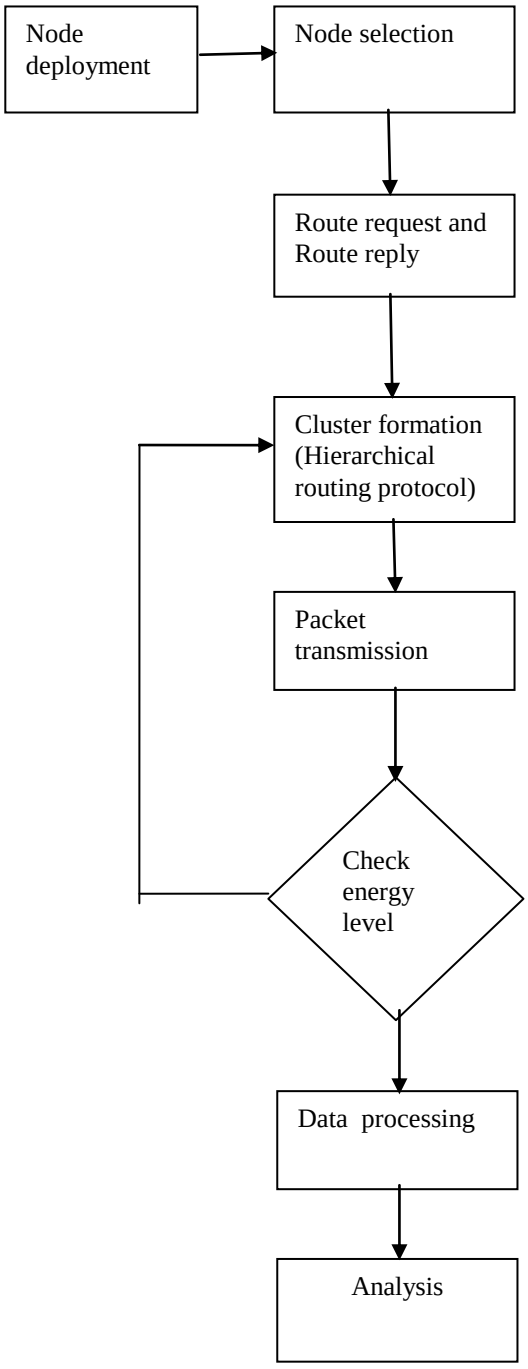


Fig.2. Flow diagram

MR-HEED pseudo code:

I. Initialize

1. $S_{nbr}\{v: v \text{ lies within my cluster range}\}$
2. compute and broadcast cost to $\in S_{nbr}$
3. $CH_{prob} \leftarrow \max\ (C_{prob} \times E_{residual} \div E_{max}, P_{min})$
4. $is_{final_{CH}} \leftarrow FALSE$

II. Repeat

1. $If((S_{CH} \leftarrow \{v: v \text{ is a cluster head}\}) \neq \emptyset)$
2. $my\_cluster\_head \leftarrow least\_cost(S_{CH})$

ISSN: 2278 – 7798

3. If(my_cluster_head = NodeID)
4. If($CH_{prob} = 1$)
5. cluster_head_msg(NodeIDfinal_CH, cost)
6. is_final_CH ← TRUE
7. Else
8. Cluster_head_msg(NodeID, tentative_CH, cost)
9. ElseIf($CH_{prob} = 1$)
10. Cluster_head_msg(NodeIDfinal_CH, cost)
11. is − final_CH ← TRUE
12. ElseIf Random $(0,1) \leq CH_{prob}$
13. cluster_head_msg(NodeID, tentative_CH, cost)
14. $CH_{previous} \leftarrow CH_{prob}$
15. $CH_{prob} \leftarrow \min (CH_{prob} \times 2,1)$

Until $CH_{previous} = 1$

III. Finalize

1. If($is_{final_{CH}} = FALSE$)
2. If($(S_{CH} \leftarrow \{v: v \text{ is a final cluster head}\}) \neq \emptyset$)
3. my_cluster_head ← least_cost(S_{CH})
4. join_cluster(cluster_head_ID, NodeID)
5. Else cluster_head_msg(NodeID, final_CH, cost)
6. Else cluster_head_msg(NodeID, final_CH, cost)

3. MODULES DESCRIPTION

MODULE 1. NETWORK PROCESS

Any device that executes programs to handle packets in a data network. In current situation, the data rates are increasing, protocols are becoming more dynamic and sophisticated. Protocols are being introduced more rapidly. There are three types of processing elements. General purpose processor, Application specific integrated circuit and Network processor. General purpose Processor is programmable but not optimized for networking applications. Application specific integrated circuit has high processing capacity, long time to develop, lack the flexibility. Network processor achieves high processing performance, programming flexibility. It is cheaper than the General purpose processor.

MODULE 2. NEIGHBOR ESTIMATION

In neighbor estimation, a HELLO message is only sent to a destination that is not in the neighbor list. This difference can provide less routing packets and therefore, better normalized routing load. The algorithm can smartly find neighbors while sending and receiving Route Request(RREQ) and Route Reply(RREP). This implementation permits the protocol to discover neighbor nodes quickly and utilize neighbor node information in the route discovery process . The node sends route request(RREQ) message to the cluster head. The cluster head is the high energy node. It sends route reply(RRPY) message to the required node.

MODULE 3. CLUSTERING AND ALGORITHM IMPLEMENTATION

The whole region is divided into several grids. This divisions are based on the transmission range of the sensor nodes. The normal sensor node is selected as a cluster, which has minimal distance from other sensor nodes within the cluster. Multi-hop routing is proposed for forwarding the data from the clusters to the sink node. There are two energy nodes. Higher energy nodes and lower energy nodes. The cluster head is the higher energy node in the cluster group. The cluster head is used for processing and sending the data. The lower energy nodes are used for sensing and sending the information to the cluster head.

MODULE 4. PATH SELECTION

Artificial bee colony algorithm is used for path selection, when the energy of the sensors in original primary path has dropped below a certain level. This allows us to distribute energy consumption more evenly among the sensor nodes in the network. Number of hope counts are also identified by using this method. The Energy Efficiency of the individual node is increased by this path selection method.

MODULE 5. ANALYSIS

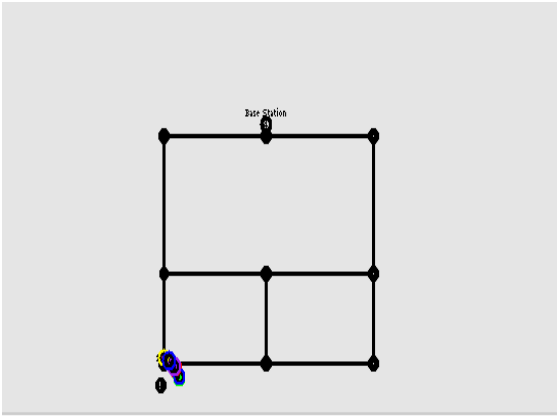
We will analysis our research to following Parameters:Packet Delivery ratio, Residual Energy, Delivery Latency. Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Graphs show the fraction of data packets that are successfully delivered during simulations time versus while the PDR is increasing in the case of DSR and AODV, AODV is better among the three protocols. Residual energy. Energy, negatively or positively charged left behind from former tenants of the home. Human auras are a powerful and potentially tangible substance. The human aura can literally extend up to three feet outside of a living body. It contains a multitude of colors, varying from red, blue, black, gray, pink and purple. The fluctuations of colors, of course, depend on many variables. If someone is angry, the aura will emit red. When someone is sad or in a very unstable mood, it tends to be gray. It glows pinks, lavenders and blues when balanced and happy. Latency and bandwidth define the speed and capacity of a network.

4.SIMULATION RESULTS

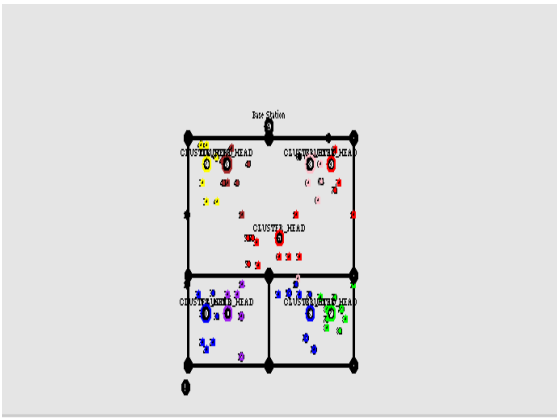
OUTPUTS

We simulate the clustering algorithm. It provides security and good quality of service. Clustering is used to avoid energy wastage and collisions that is occurred between the nodes. Fig(a)shows the node creation and initialization of the clustering process. Fig(b)the cluster formation of the network process. The cluster head is selected by using residual energy and throughput. The cluster head is formed by using hierarchical routing protocool. Fig(c)shows the informations are exchanged among the nodes using clustering technique. The cluster head collects the information from the cluster member and send that information to the base station for performance analysis. Fig(d)relationship between simulation time and consumption energy. Fig(e)relationship between simulation time and lifetime. Fig(f)relationship between simulation time and packet received. Thus the packet delivery ratio is high in this network process. It is the ratio of data packets received by the destinations to those generated by the sources. Fig(g)throughput using clustering.

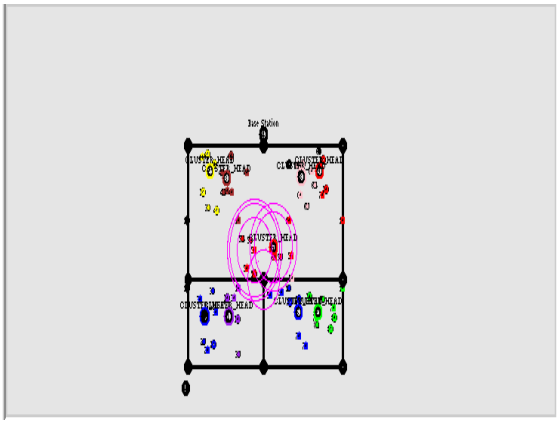
ISSN: 2278 – 7798



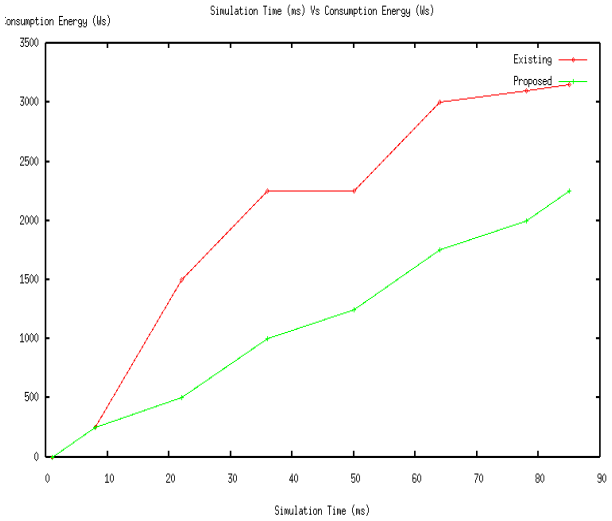
(a)Node creation and initialization



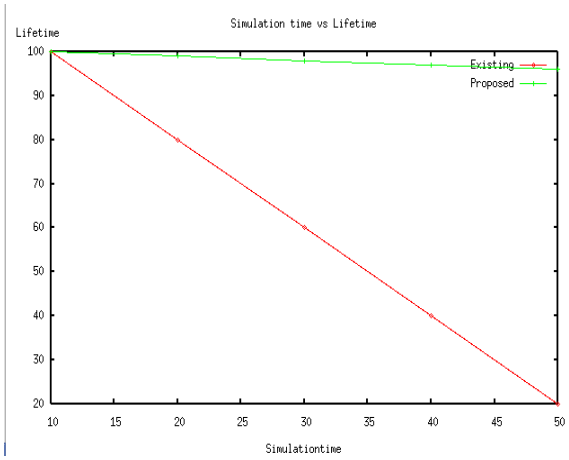
(b)Cluster formation



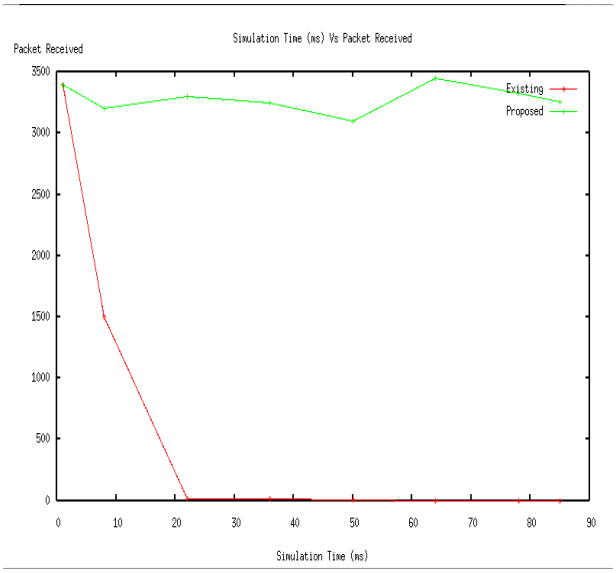
(c)Informations are exchanged among the nodes using clustering



(d)Simulation time vs Consumption energy

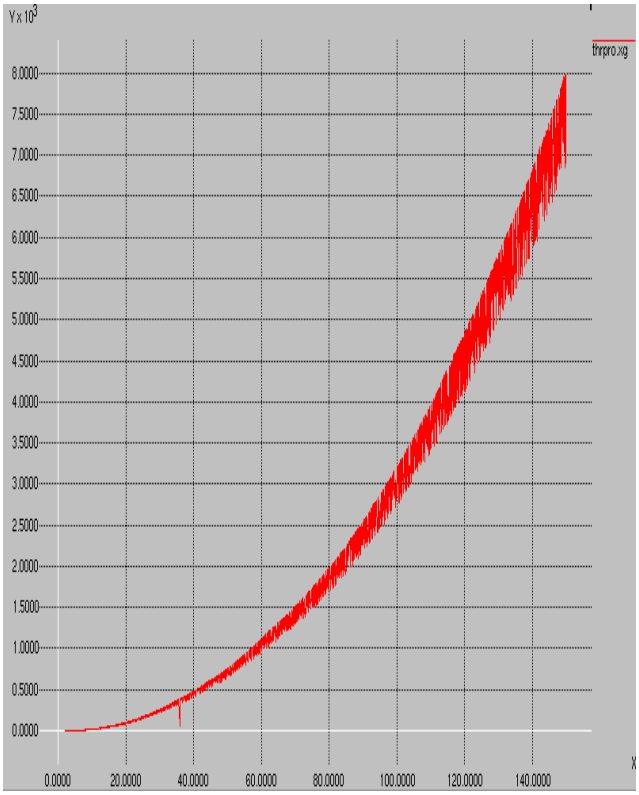


(e)Simulation time vs Lifetime



(f)Simulation time vs Packet received

ISSN: 2278 – 7798



(g) Throughput using clustering technique

Fig.3. Output shots

5. CONCLUSION

We have shown that the recent advances in rate less coding and decoding can be profitably exploited to achieve a robust and resource location technique in Grid systems. The major novelty of the proposed approach lies in the use of network coding principles in a scenario where local data can be updated asynchronously. We have proposed Clustering technique which improves the security and QOS. If the number of data is less than the number of cluster then assign each data as the centroid of the cluster. Each centroid will have a cluster number. If the number of data is bigger than the number of cluster, for each data, we calculate the distance to all centroid and get the minimum distance. This data is said belong to the cluster that has minimum distance from this data. Since we are not sure about the location of the centroid, we need to adjust the centroid location based on the current updated data. Then assign all the data to this new centroid. This process is repeated until no data is moving to another cluster anymore. Mathematically this loop can be proved convergent. Then it will be including the security algorithm that's elliptical curve cryptography security algorithm using in our proposed system. The MR-HEED clustering procedure will be introduced in our proposed system.

4. SCOPE OF FUTURE WORK

In our proposed system using the elliptical curve cryptography algorithm for the sensor network. It will be more secure and network life time of the network will be increasing. The collision is greatly reduced by using this algorithm. Security is increased by using the elliptical curve cryptography algorithm. Quality of service parameters is increased. The comparative Analysis is given here to show the difference between the existing and the proposed method. But our future enhancement will be the various proactive or reactive protocol is there and to implement all other routing protocol and compare it then analysis the result. After that will introduce the trust based routing protocol for the future enhancement, after that introduce a cluster based transmission in future level enhancement work. To get the better result with several protocols can do the analysis with the Protocols like DSR and DSDV. The comparative calculations are verified by the Graphical outputs.

REFERENCES

[1] M. Adler, Y. Bartal, J.W. Byers, M. Luby, D. Raz. A, "Modular Analysis of Network Transmission Protocols" Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems, June 1997.

[2] Abbasi, A. A., &Younis, M., " A survey on clustering algorithms for wireless sensor networks," Computer communications, 30(14), 2826-2841. 2007.

[3] Akkaya, K., &Younis, M., " A survey on routing protocols for wireless sensor networks," Ad hoc networks, 3(3), 325-349. 2005.

[4] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., &Cayirci, E., " Wireless sensor networks: a survey," Computer networks, 38(4), 393-422. 2002.

[5] L. Alvisi, et al., "How Robust are Gossip-Based Communication Protocols?" Operating Systems Rev., vol. 41, no. 5, pp. 14-18, Oct. 2007.

[6] N. Carvalho, J. Pereira, R. Oliveira, and L. Rodrigues, "Emergent Structure in Unstructured Epidemic Multicast," Proc. 37th Ann. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN '07), pp. 481-490, 2007.

[7] Islam, K.," Energy aware techniques for certain problems in Wireless Sensor Networks," (Doctoral dissertation, Queen's University). 2010.

[8] M. Jelasity, A. Montresor, and O. Babaoglu, "Gossip-Based Aggregation in Large Dynamic Networks," ACM Trans. Computer Systems, vol. 23, no. 3, pp. 219-252, Aug. 2005.

[9] A. Kermarrec, L. Massoulie, and A. Ganesh, "Probabilistic Reliable Dissemination in Large-Scale Systems," IEEE Trans. Parallel and Distributed Systems, vol. 14, no. 3, pp. 248-258, Mar. 2003.

[10] P. Trunfio, D. Talia, H. Papadakis, P. Fragopoulou, M. Mordacchini, M. Pennanen, K. Popov, V. Vlassov, and S. Haridi, "Peer-to- Peer Resource Discovery in Grids: Models and Systems," Future Generation Computer Systems, vol. 23, no. 7, pp. 864-878, 2007.

[11] R. van Renesse, D. Dumitriu, V. Gough, and C. Thomas, "Efficient Reconciliation and Flow Control for Anti-Entropy Protocols," Proc. Second Workshop Large-Scale Distributed Systems and Middleware (LADIS '08), 2008.

[12] V. Vijayakumar, R.S. Wahida Banu, and J.H. Abawajy, "An Efficient Approach Based on Trust and Reputation for Secured Selection of Grid Resources," Int'l J. Parallel, Emergent and Distributed Systems, vol. 27, no. 1, pp. 1-17, 2012.

ISSN: 2278 – 7798

BIOGRAPHY

J.Sebastina Queen Rose,
Department of ECE,
Pavendar Bharathidasan College of Engineering and Technology,
Thiruchirapalli, Tamilnadu, India.

S.Sumithra,
HOD of ECE,
Pavendar Bharathidasan College of Engineering and Technology,
Thiruchirapalli,Tamilnadu, India.

ISSN: 2278 – 7798