International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN: 2456-172X | Vol. 4, No. 3, September - November, 2019 | Pages 75-86

EFFICIENT SOURCE BALANCED ROUTING PROTOCOL TO ENHANCE QoS FACTORS IN DISRUPTION TOLERANT NETWORKS

S.Jagan, Associate Professor, *Department of CSE, Agni College of Technology, Chennai, India*

Abstract

Disruption Tolerant Networks consists of nodes that are randomly deployed in the network. Due to the random deployment of nodes, enhancing the Quality of Service of the network becomes more difficult. The coverage of the network also becomes an issue due to the movement of the nodes. Handling the fault nodes in the network and Data traffic balancing are the other issues that occur in Disruption Tolerant Networks. The network overhead increases due the traffic flow of data in the network. To overcome all the above issues, Efficient Source Balanced Routing is used. The Efficient Source Balanced Routing enhances Quality of Service factors that include Throughput, Overload and Packet Delivery Ratio by handling the fault in the Disruption Tolerant Network. The node density is measured by ranking the nodes that enables in handling the nodes for data transmission and thereby increases the performance of the network. Source Encoding is done to provide Lossless Compression in the network. Quality of Service Distributed Routing protocol is compared with Efficient Source Routing which is the proposed work to overcome the security issues and the Quality of Service factors are satisfied in the network.

Keywords- Quality of services (QoS), Efficient Source Balanced Routing, Disruption Tolerant Network, Node Density, Epidemic Routing, Source Encoding.

I. INTRODUCTION

Disruption Tolerant Networks makes use of a mechanism to transfer the data from source node to destination node. Store-Carry-Forward method is implemented where the data is stored in the buffer and then carried around until it gets contacted with another node and finally it forwards the data when the node comes in contact with another node. Due to the frequent disconnections between the nodes, it is a challenging task to design an efficient routing protocol. Various protocols have been proposed in improving the Quality of Service in the DTN network.

Efficient Source Balanced Routing Protocol:

Disruption Tolerant Networks consists of nodes whose topology and parameters changes with time. They are more important because their applications are used in traffic planning and finding the route. In Disruption Tolerant Networks various old routing techniques have been proposed to improve the Quality of Service of the network and they are not applicable due to the challenging issues in DTN. When compared to the other routing techniques the proposed Efficient Routing technique balances the mitigation of attack among all the nodes. The ESBR protocol maintains the nodes trust value in which the node behaves as expected. The nodes trust value is calculated from the nodes past behaviors and from which the future behavior of the nodes can be predicted.

Trust Management Model:

Trust Management Model not only improves the Quality of Service of the network but also includes the trust properties such as honesty and unselfishness. The model avoids the frequent disconnections in the network thereby increasing the QOS.

Fault Tolerance and Coverage constraints:

Fault Tolerance and Coverage constraints are one of the critical issues in DTN due to the nodes with high energy consumption. When the capability of routing becomes difficult, the coverage problem arises and the node becomes the fault node in the network. Various issues like packet loss, network overhead and throughput arises in this technique.

II. PROBLEMS IN INCREASING QUALITY OF SERVICE IN DTN NETWORKS-EXISTING WORK

A. Coverage problem:

Due to the failure of routing capability of the node in the DTN Network, the coverage problem arises that leads to disconnection between the nodes. The nodes then become the fault nodes. Optimization of Network configuration and deployment model is being done to handle the fault nodes. Though the model gives us a solution, it has few drawbacks that include packet loss, network overhead and throughput and the Quality of Service constraint becomes the major problem.

B. Fault tolerance problem:

The nodes in the network become fault node due to the routing problems that does not allow data transmission and becomes the failure node in the network. The nodes in the DTN Networks consume high energy to transmit the data and hence when limited energy is not consumed by the node, then the node becomes the fault node in the DTN Network

C. Data loss:

Due to the entries of malicious nodes in the network, nodes tend to loss the data transmitted by the previous nodes. The loss of data leads to the decrease in packet delivery ratio and

Quality of service is not guaranteed in the network where the data cannot be transmitted in a secure way in the Disruption Tolerant Networks.

D. Limited energy:

When more is the data transmission rate, the energy consumption becomes more. The energy required for communication is high when compared to processing the data. Data Aggregation helps in reducing the communication process but the Quality of data gets affected and thereby the performance of the network decreases.

III. METHODS TO INCREASE THE QUALITY OF SERVICE FACTORS IN DTN NETWORKS-EXISTING WORK

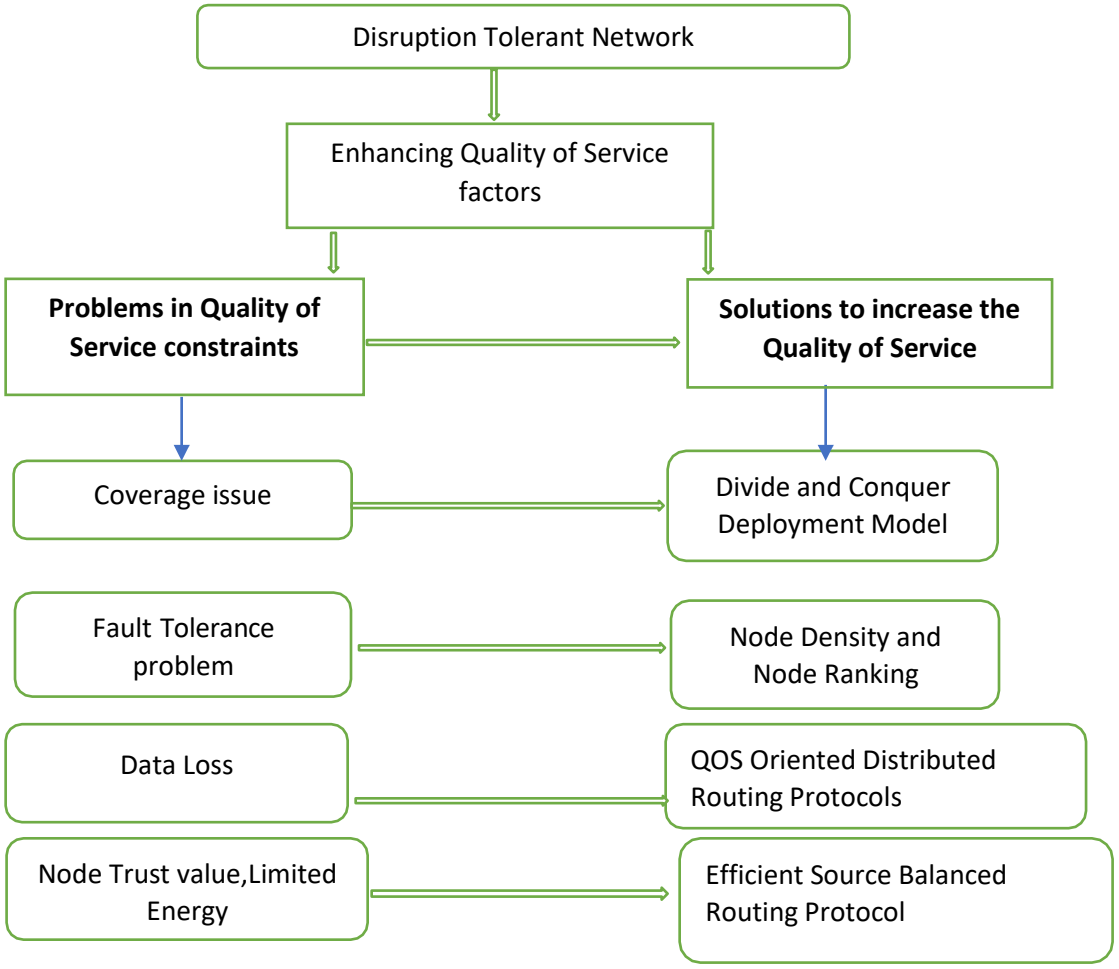

Figure1. Enhancing Quality of Service factors in Disruption Tolerant Networks

A. The divide and conquer deployment model based on triangular form:

The divide and conquer deployment model help in solving the coverage problem in the social networks. The model provides us a sufficient sensing of the coverage issues. When the nodes undergo deployment mode, high degree of node capabilities arises and due to the high data traffic rate and also due to the interference each node undergoes exhaustion of energy. In order to overcome the issues in deployment model the routing strategies are invoked in the Disruption Tolerant Networks that tends to improve QOS constraints.

B. Node Density:

The nodes are being clustered based on their density and space of the node in order to balance the traffic using spatial and temporal data. To handle the fault node in the network, cooperative caching of the node information is enabled and thereby the density of the node is calculated in the Disruption Tolerant Networks by increasing the Quality of Service.

C. Node Ranking:

By calculating the density of the node alone cannot improve the network efficiency due to the presence of malicious nodes in the network. It is important to rank the nodes based on calculation of node density and thereby the data can be transmitted effectively. The malicious nodes can be avoided by using Source Encoding Algorithm that compresses the data transmitted and provide a lossless compression by eliminating the space and time complexity in the network. The redundant bits in the data are transmitted due to the lossless compression and therefore the QOS Constraint is enhanced in the network.

D. Puzzle based Data anonymous routing method:

The compressed data is encrypted using the Puzzle based Data anonymous routing in order to transmit the data securely by encoding them and thereby avoiding packet loss and data compression attack without disturbing the routing

E. Epidemic routing:

The most frequently used mechanism for fault tolerance is the Epidemic routing. Many optimization techniques are carried out in Epidemic routing to monitor the nodes in the network for high data delivery by reducing the communication cost. The nodes are selected based on the density of the nodes.

IV. DATA ADVERSE ROUTING FRAMEWORK-PROPOSED WORK

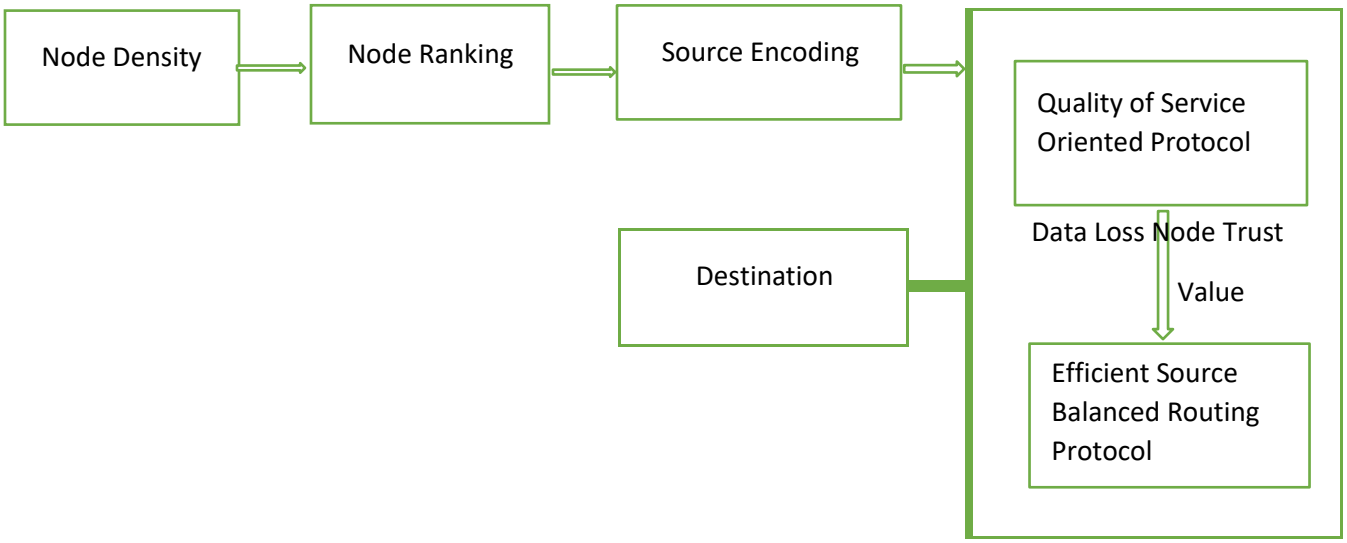

Figure2. Data Adverse Routing Framework

1. **Prediction of Density of Node in Quality of Service factor:**

The Density of the node is calculated based on connections. When the number of nodes connected is more, and then the density of the node becomes high.

Pseudo code for Node Density prediction based on QOS factors

1. Set of Nodes = [N1,N2,N3...Nn]
2. Energy of Nodes = {E1, E2, E3...En}
3. Estimation of Node energy based on distance

$$E_i=E_t\,(K-i+1)+E_r\,(K-i)+E_{id}$$

Where

E_r – Energy required by the packet at particular node

E_{id} - Energy spent per second

K - No. of Partition of the data into packets

4. Node energy based weight or queue is given by

$$\mathbf{W_v = w_1\Delta_v + w_2D_v + w_3M_v + w_4P_v}$$

5. Energy required per second for successful transmission of a data packet E_t

$E_t = e_t + e_d d$ where

e_t - energy dissipated in the mode per packet per second

$e_d d^n$ -the amount of energy required per packet per second

n -path loss exponent

6. The Energy utilization or node density calculated as follows

$$E_U = (E_{used}/E_t)*100$$

Where

E-total energy utilized by the network during its lifetime

ET -total energy of the nodes at the time of deployment

Table 1 -Simulation Parameters used to build a protocol

Simulation Parameter	Value
Simulator	NS2
Topology Size	1000m *1000m
Number of Nodes	195
Bandwidth of the Network	2Mbps
Traffic type	CBR

2. **Prioritization based Node Ranking:** The Ranking of nodes are based on Prioritization. The Prioritization is based on data and energy of the node. The nodes are selected for cluster head based on their energy constraints and their distance from the Base station. The energy of the node can be saved by calculating the distance of the node from the base station. Prioritization base Node Ranking ensures that all the nodes in the network can be reached through the connected Cluster Heads and thereby solving the problem of coverage in Disruption Tolerant Networks.

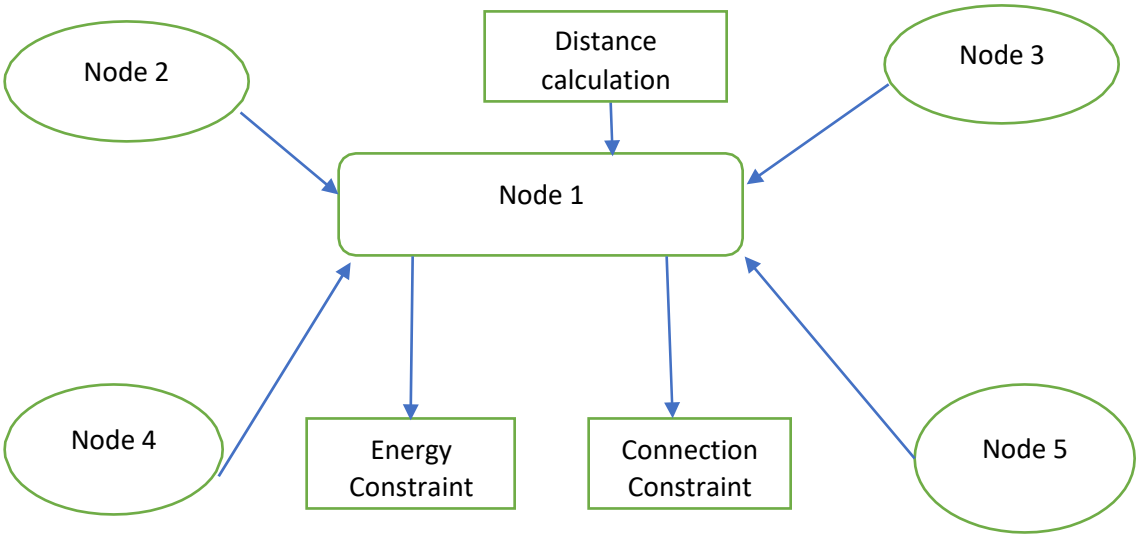

Figure3. Prioritization based Node Ranking

3. **Lossless Compression based Source Encoding:**

Source Encoding is done using Shannon –Fano Compression Technique which provides a lossless compression. The technique provides least possible bits for the most possible bits for the source code. Set of probabilities are used and is compared with the similar occurrences before the data is transmitted in the Disruption Tolerant Networks.

4. **QOS Oriented Distributed Routing Protocols:**

Quality of Service protocol manages the data traffic thereby reducing packer loss, latency. The QOD Protocol manages the network resources on the Disruption Tolerant Network.

5. Efficient Source Balanced Routing Protocols:

The Efficient Source Balanced Routing Protocol balances the mitigation of attack among all the nodes. The ESBR protocol maintains the nodes trust value in which the node behaves as expected. The nodes trust value is calculated from the nodes past behaviors and from which the future behavior of the nodes can be predicted.

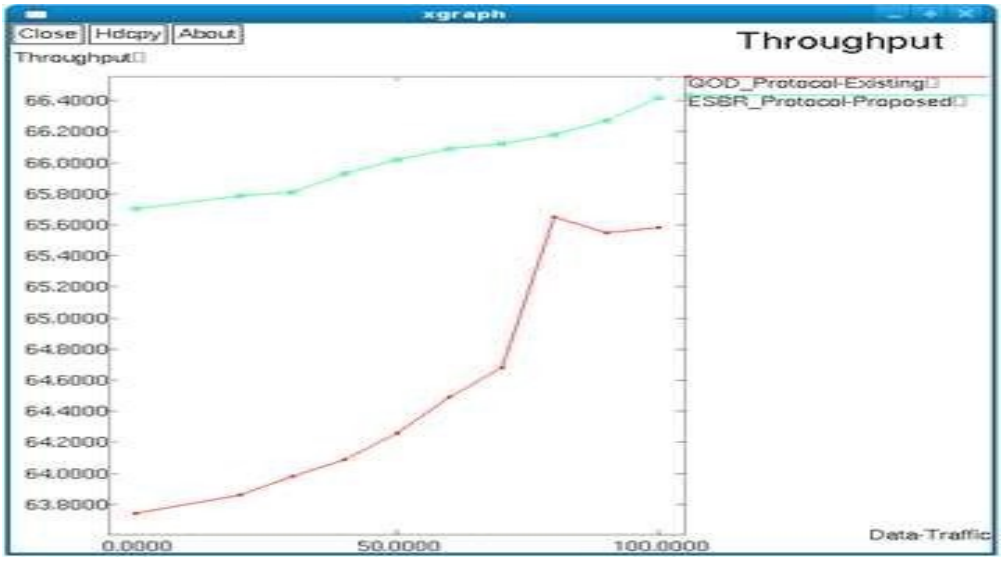

Figure4. Analysis of Throughput using QOD and ESBR protocols

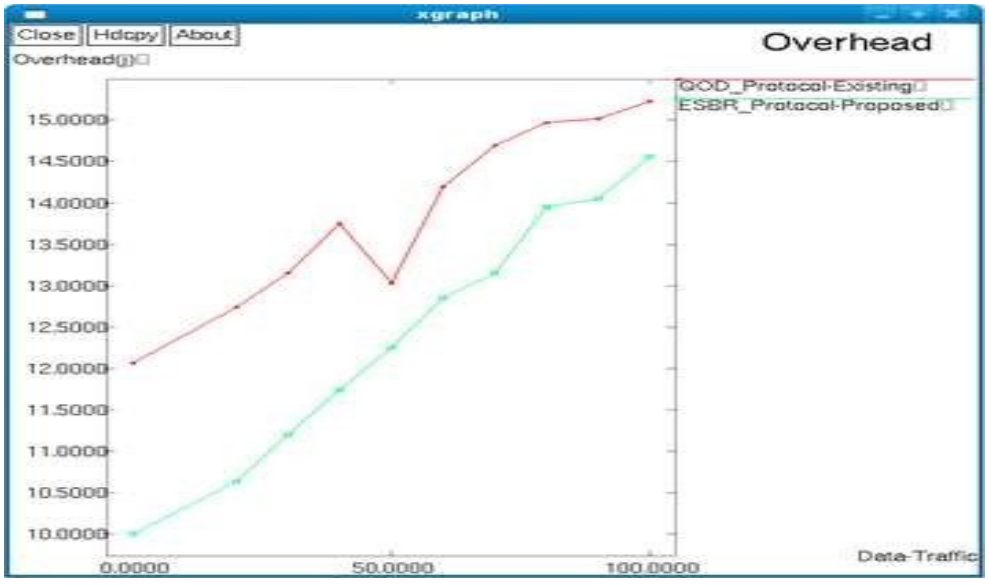

Figure5. Analysis of Overhead using QOD and ESBR protocols

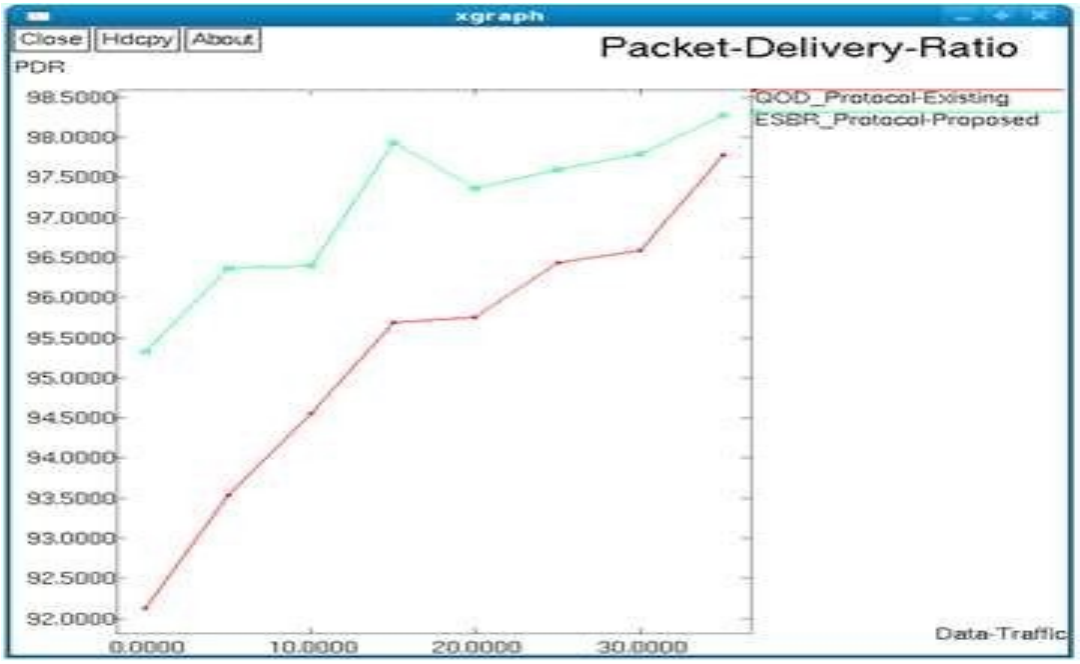

Figure6. Analysis of Packet Delivery Ratio using QOD and ESBR protocols

Table 1 – Performance Evaluation of the protocols considering Quality of service factors

Technique	Throughput	Overhead	Packet Delivery Ratio
QOD Protocol- Existing	65.58	15.23	97.78
Efficient Source Balanced Routing Protocol Proposed	66.42	14.56	98.28

V. CONCLUSION

The Proposed model is designed in such a way that various Quality of Service factors are considered. The energy of the node is estimated by calculating the node density based on number of connections and ranking the nodes based on Prioritization for efficient transmission of data. Data compression is also achieved by Source Encoding which provides a lossless Compression. Finally the data is provided with security through Efficient Source Balanced Routing Protocol that tends to improve the Quality of Service factors that includes the node energy, Lossless Data, Handling Fault Nodes and Coverage issues in Disruption Tolerant Networks. The proposed

protocol is compared with various existing protocols regarding the Quality of Service factors including Throughput, Network Overhead and Packet Delivery ratio and it is proved to be much better than the existing protocols which enhance the Quality of Service factors. Thus the network performance is increased in a Disruption Tolerant Networks.

VI. REFERENCE

[1] K.Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment- based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2015. 12. B.Awerbuch, D. Holmer, C.-N. Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in Proc. ACM WiSe, 2012, pp. 21–30.

[2] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks,"IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[3] D.S.NishantChaurasia, Sanjay Sharma, "Review study of routing proto-cols and versatile challenges of manet",vol.1

[4] S. Ioannidis, A. Chaintreau, and L. Massoulié, "Optimal and scalable distribution of content updates over a mobile social network," in Proc. IEEE INFOCOM, Rio de Janeiro, Brazil, Apr. 2009,pp. 1422–1430.

[5] T. Karagiannis, J.-Y. Le Boudec, and M. Vojnovi_c, "Power law and exponential decay of inter contact times between mobile devices," in Proc. 13th Annu. ACM Int. Conf. Mobile Comput. Netw., 2007,pp. 183–194.

[6] Q. Li and G. Cao, "Mitigating routing misbehaviors in disruption tolerant networks," IEEE Transaction on Information Forensics and Security, vol. 7, no. 2, pp. 664-675, April 2012.

[7] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in In Proceeding IEEE 5th international conference on Communication System and Networking, 2013, pp. 1-7.

[8] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," Elsevier J. Ad Hoc Networking, vol. 14, pp. 1497–1509, 2013.

[9] PreetiNagrath,AshishKumar,ShikhaBhardwaj, "Authenticated Routing Protocol based on Reputation System For Adhoc Net-works",International Journal on Computer Science and Engineer-ing(IJCSE),Vol.2: 3095-3099,2010

[10] Seunghun Cha, Elmurod Talipovand Hojung Cha. Data delivery scheme for intermittently connected mobile sensor networks.0140-3664,2012, Elsevier.