# Performance Analysis of CAT Swarm Optimization Algorithm in Disruption Tolerant Networks

DOI:10.36909/jer.11327

**R.Sangeetha[*], Dr.R.Vijayabhasker[**]**

*[*]Ph.D Scholar, Faculty of information and Communication Engineering, Anna University, Regional centre, Coimbatore, India*

*[**] Assistant Professor, Department of Electronics and Communication Engineering, Anna University, Regional centre, Coimbatore, India*

*Email:[*] sangeethasivakumarphd@gmail.com , [**]kaviji04@gmail.com*

## ABSTRACT

Disruption tolerant networks (DTN) are networks that provide unguided technologies. Solar technologies and Radio frequencies are used to operate the network. In DTN networks the connectivity does not last for a long time and they do not provide end to end connectivity. Therefore it uses store and forward technique to forward the packets to the destination nodes. When N number of nodes is participating in the network, each node receives packets from the previous node and sends acknowledgment to the sender node. Time delay occurs on receiving and sending acknowledgment continuously. Collision occurs due to the congestion in the network. Due to the irregular connectivity in the network, the compromised nodes try to drop the whole packet or part of the packet. The Blackhole and Greyhole attacks occur due to the packet loss. Optimized algorithm can be used to solve the above attacks. By using CAT Swarm optimization algorithm, the attacks can be prevented and it minimizes the Time delay in delivering the packets.

**Keywords-**Disruption Tolerant Networks, Blackhole, Greyhole, Time delay, Collusion

## INTRODUCTION

In Mobile Ad-hoc networks the data is split into packets and are forwarded to the next node only when there is a link between the two nodes. Packet loss occurs when the establishment fails between the two nodes. Therefore the packet delivery ratio decreases. In order to overcome the above issue the Disruption Tolerant Networks are introduced. Packet loss due to link establishment does not occur in Disruption Tolerant Networks due to its packet storing capability. DTN works better in uncertain terrestrial regions. Continuity in connection does not last for a long time in DTN networks. End to end connection does not exist in Disruption Tolerant networks. DTN follows store-carry-forward method using set of protocols. Each node stores the packet it receives until it contacts some other node. Storage is also another main issue in DTN networks. Time delay occurs when the packets are not delivered.

### 1. *Challenges in Delay Tolerant Network*

Disruption Tolerant Networks are more efficient in providing high packet delivery ratio by using store and forward method. Though they provide better ratio in packet delivery, it has to handle few issues that include node contact and storage issues in nodes.

1.1 Contact between nodes:

The nodes in the Disruption Tolerant Network gets in contact with each other only at a particular period of time. The nodes exchange the packet at that point of contact. The message transfer is more difficult when the nodes are moving since the wireless channels are dynamic in nature. The process of message transfer is a difficult process in the case of nodes that transfer to various locations. The nodes will have to be identified in the network and then the message is being transferred. Duration in contact and inter-contact time are the essential parameters in transferring the packets.

1.2 Storage issue in nodes:

Each node has to maintain a buffer to store the packets. The buffer of each node continues to store the packet until it gets a contact with another node. The buffer since it keeps on storing the packets, the storage space increases. As the storage space increase, the functionality of that particular node increases. Therefore the node has to transfer more number of packets at that period of time. When the node fails to transfer the packet at that period of duration, the packet delivery ratio decreases. Routing can provide a better solution to the problem of storage. The overhead issue in storage includes:

i. End to end connection does not occur in delivering the packets at all period of time.

ii. The routing protocol does not support at all times.

iii. The topology of the network are ignored.

## 1.3 Requirements for security in DTN:

Disruption Tolerant Network requires certain security requirements since the network does not provide end to end connectivity they include:

### 1.3.1 Authentication

It is necessary to check for the authenticity of the packet since some nodes may misbehave. The legitimacy rate of the packet must also to be checked.

The class of service the nodes provide. The packet has to be analysed for its authenticity since the packet has to received from the authenticated source and has to reach the authenticated destination.

### 1.3.2 Integrity**:**

The integrity of the message ensures that the contents of the message are not altered. Each node has its responsibility to safeguard the message without alteration so that the destination node can view the message without any confusion. The issue in integrity of the message includes message modification, message falsification and replay attacks in the DTN networks.

### 1.3.3 Confidentiality:

The confidentiality of the message ensures that the message is not revealed to the third parties who are unauthorized. The unauthorized node tends to view the content of the message during the process of bundle propagation in DTN links.

### 1.3.4 Privacy:

The privacy of the node ensures that the location of the node is not revealed to the other nodes and also the node with which it communicates. The nodes in the network has to maintain its privacy since misbehaving nodes may try to find the location of the sender, receiver and the intermediate nodes during message transfer.

## RELATED WORK

### *Reliability-redundancy problem:*

Reliability refers to the cost, weight and volume of the system. Reliability problem is addressed by the new scheme called cat swarm algorithm. It is an optimization technique that follows the behaviour of a cat. The CSO algorithm is modelled based on the strong curiosity on the moving objects and the skill on hunting. They are called the seeking mode where the moving object is targeted by the cat when the cat is at rest and the tracing mode where the cat begins to hunt its prey while it begins to move.

### *Butterfly Optimization Algorithm:*

The butterflies make use of sense receptors to locate their food. The sensing receptors are spread all over their body for the other butterflies to sense them. The butterflies act as searching agents and they perform optimization. Each butterfly emits fragrance so that the other nearby butterflies can sense them in that particular region. Each butterfly has its own intensity. When a butterfly changes its location, the fragrance will vary. A butterfly when receives greater amount of fragrance than its own fragrance, then it starts moving towards the butterfly that has emitted ore amount of fragrance. Each butterfly has its own amount of fragrance that are called fitness fragrance of the butterfly. The butterfly moving towards the greater fragrance are called global search. When a butterfly does not sense any fragrance greater than its own fragrance, then the butterfly move randomly and are called local search.

*Data clustering using cat swarm optimized algorithm:*

The clustering is based on grouping N number of objects. The clustering is done by supervised learning or unsupervised learning. In supervised learning ,the objects are grouped on mentioning the number of classes by the training data. In unsupervised learning the objects are clustered automatically and the training data need not specify the number of classes. Here in data clustering, n number of objects are allocated to each cluster and the distance between the object and the centre of the cluster are measured which are called distance measurement. The main goal of optimization technique in data clustering is to find out the centre of clusters.

*Data prediction and optimized clustering:*

The properties involved in clustering are homogeneity and heterogeneity. In homogeneity clustering, the objects that belong to the same cluster has similar properties. In heterogeneity clustering, the objects that belong to different clusters have different properties. Thus by effective grouping, the optimal solution is found .

*Ant colony optimization algorithm:*

Ant colony optimization algorithm deals with grouping the ants in the environment which can provide an optimized solution. The algorithm finds out the shortest path to reach the destination point from the source point. Here in ant colony optimized algorithm, the ant finds out the shortest path between the shelter and food resource point. The ant when moving secrets a chemical substance called pheromone indicating that it travels along the path where the food resource is available. The ant secrets the substance so that the other ants could follow along the path where the food is available. Thus the shortest path is found by the real ants by secreting the pheromone between the source and destination point.

*Particle swarm optimization algorithm:*

The particle swarm optimized algorithm deals with the velocity and position of the particle. The particles travel along the search space with their own experience they gained and the experience of the other neighbours. Each time when the particle traverse along the path, the velocity and the position of the particle are updated. The process of the particle travelling along the path with its own velocity and its current position and updating the velocity and position of the particle keeps on repeating until an optimized solution is obtained thereby increasing the performance of the network.

*Discrete binary cat swarm optimized algorithm:*

The binary cat swarm optimized algorithm varies from the cat swarm algorithm in such a way that it consists of values in zeros and ones. The Binary CSO also consists of two modes as in the case of CSO that includes seeking mode and tracing mode. As usual, in seeking mode the cats are in resting mode but the current position of the cats in the swarm slightly varies. When the current position of the cat changes, the values are assigned as zeros and ones. The parameter SRD(Seeking range of selected dimensions) in the original CAT swarm optimization algorithm is replaced by the parameter PMO(Probability of mutation operation) in the Binary CSO.

*Seeking mode of BCSO:*

1. If the Boolean flag indicates true, then the original position of the cat might be the member and so the SMP copies of the current position of the cat will have to be taken additionally and the current position of the cat will be taken as one of the member. If the Boolean flag indicates false, then produce SMP copies of the current position of the each cat.
2. Select as many as CDC dimensions for each SMP copies produced and the CDC dimensions are mutated according to the PMO(probability of mutation operation) and the old ones are replaced.
3. The fitness value of all the members are found by considering the cost function.

4. If the fitness values are similar, then similar probability is assigned to all of the members. If the values are not similar, then the selected probability of each member has to be calculated.
5. One of the candidate is selected and the current position of the candidate is replaced with the selected candidate.

*Tracing mode of BCSO:*

The main function of the tracing mode in BCSO is that the cats are moving towards the best target. The velocity is defined differently in CSO and BCSO. In CSO, the velocity shows the difference between the current position of the cat and the previous position of the cat. In BCSO the velocity defines the probability of mutation of each dimension of the cat.

The research gap of this optimized route establishment is reviewed by various literatures. The problem is about security, reliability and storage issue. The cloud based model overcomes the storage issue by gig data analysis procedure. Authentication process improves the performance result of security. All this makes to get reliable communication model. This research motivates to increase the performance of optimized route establishment in big data analysis and cloud model.To improve the security, reliability and large storage issues, the proposed cat swarm optimization is developed.

## CAT SWARM OPTIMIZATION ALGOTITHM

Cat Swarm optimization algorithm is an optimizing algorithm that deals with the behaviour of cats. It naturally consists of two modes that includes seeking mode and tracing mode. The two modes are used for the movement of cats in the solution space. The number of cats participating in the seeking mode and tracing mode in one iteration are fixed as a ratio called MR.

*Parallel cat swarm optimization algorithm:*

1. Exchange of information:

The cats are sorted by their fitness values for every cluster. A near best solution is randomly chosen from the clusters and the cat having the worst fitness value is replaced. The cat and the nearest best solution must not emerge from the same cluster. The above process is repeated for all clusters.

2. Parallel tracing process:

   In Parallel tracing process, the cats are grouped into clusters. The cats in one cluster does not get affected by the other cats that belong to another different cluster. The cats have the power to only share their own nearby best solution with the other clusters.

*Four essential parameters in the seeking mode of CSO:*

1. **Seeking memory pool(SMP):**

   SMP defines the size of the memory of each cat. The parameter varies for different cats.

2. **Seeking range of selected dimensions(SRD**): SRD defines the mutation ratio of the dimensions.
3. **Counts of dimensions to change(CDC**):

   CDC defines the number of dimensions to be varied.

4. **Self-position considering(SPC):**

   SPC is a Boolean flag that decides whether the current position of the cat is the one that has to be moved to or not.

*Seeking mode of CSO:*

1. When the Boolean flag is set to one, then many SMP copies of the position of the cats are produced but only the current position of the cat will be taken as the member in the cat swarm. If the boolean flag indicates zero, then produce SMP copies of the current position of each cat.
2. For each copies taken produce CDC dimensions and either add or subtract the SRD percents of the current values and the old values will have to be replaced randomly.
3. The fitness value of all the members of the cat swarm is evaluated.

4. If the fitness values if all the cats seems to be identical, then the probability has to be assigned for each cat.
5. The current member of cat swarm is replaced with the selected member.

*The tracing mode of CSO:*

The main function of the tracing mode in CSO is that it tries to trace the target position**.** The velocity of the cat and the best position of the cat are the two factors that help us to determine the next movement of the cat. The parameters of tracing ode include

1. Updating the velocities of each cat at varying dimensions.
2. The velocities of each cat has to lie within the bound. In case if the velocities are not within the bound, then the limit has to be set.
3. Updating the position of the cats.

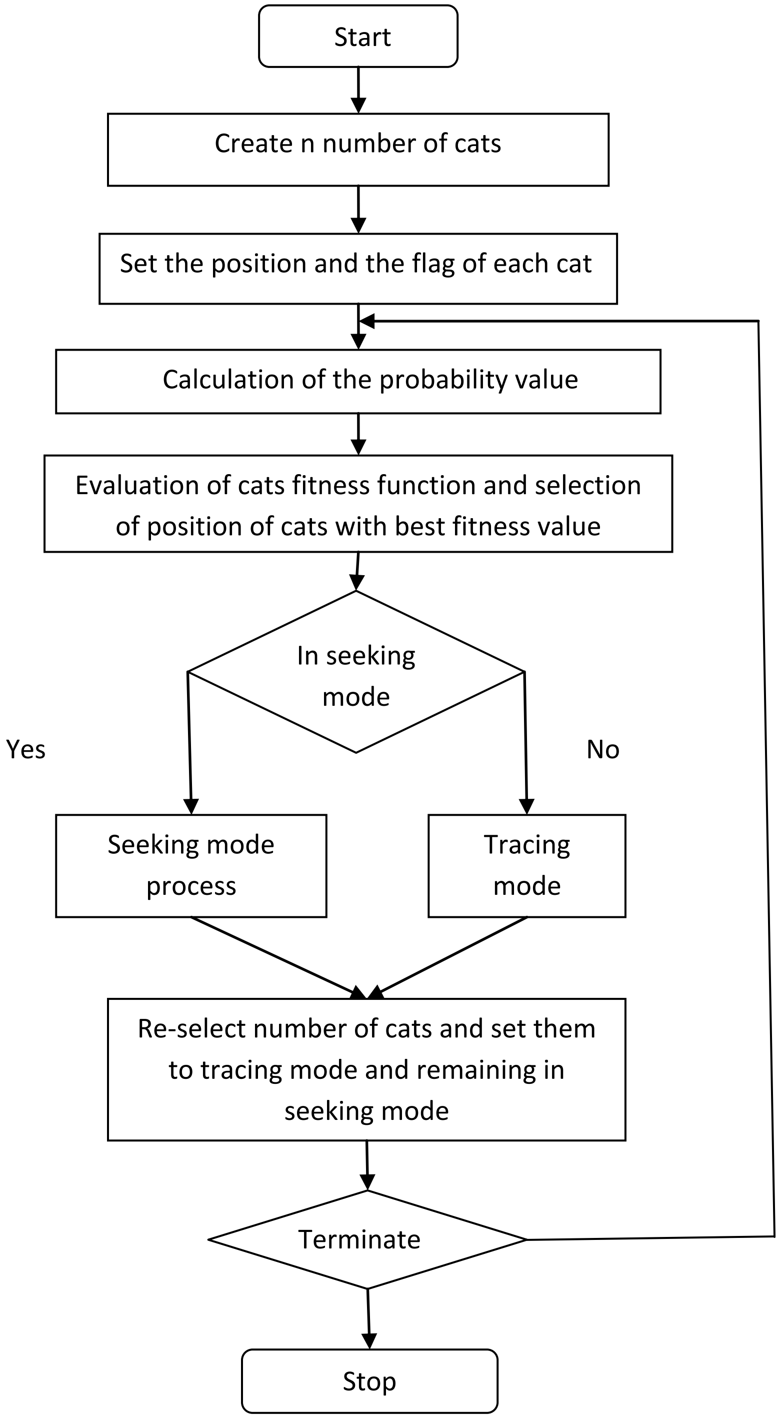

Start
Create n number of cats
Set the position and the flag of each cat
Calculation of the probability value
Evaluation of cats fitness function and selection of position of cats with best fitness value
In seeking mode
Yes
No
Seeking mode process
Tracing mode
Re-select number of cats and set them to tracing mode and remaining in seeking mode
Terminate
Stop

**Fig 1:** Flow chart of Cat Swarm Optimization

Initially n number of cats is created. The position of the cat and the flag are set. The probability value is calculated. The fitness function of each cat is evaluated and the positions of the cats with the best fitness value are selected. The cat swarm algorithm has two process that includes Seeking mode and

Tracing mode. When the cats are in seeking mode, they are set to be in rest and when in tracing mode, they move in search of the prey. The cats are analysed whether in seeking or tracing mode. The cats when in seeking mode, they tend to be in rest but they keep on noticing the environment. When the cats are in tracing mode, they begin to move to search for its prey. The cats are again selected and put into the tracing mode and the remaining in seeking mode. The process thus stops and if not terminated, then the process continuous by again setting the position and flag of the cats.

## PROPOSED WORK

1. *Cat Swarm Optimization Algorithm in DTN:*

Routing misbehaviour is one of the major problem in Disruption Tolerant Network. The selfish nodes tend to participate in the network by refusing to transfer the data packet to the destination nodes. They try to behave like the normal node in the discovery of routes and route maintenance process. The selfish nodes may choose the route chosen by the source node to transfer the data packet. In the TCP protocol, the route when found to contain selfish nodes, an alternate route is chosen and the data are forwarded. The selfish nodes again try to find the alternate route and deny the packet transmission. Since the source node does not have any knowledge, the source node concludes that the route is unavailable to transfer the data packet. The confusion leads to network failure and no proper communication channel is provided to the source node. The selfish nodes terminates the data traffic flow. The main problem that is being identified in the network is that the source node does not have any knowledge about the activities in the network. A proper communication channel should be provided to the source node by using authenticated acknowledgement scheme. The Cat Swarm Optimization Algorithm prevents the selfish nodes from the route that has been selected by the source node for data packet transfer. The authenticated acknowledgement scheme gives standard route of two hopes (three nodes) in the opposite direction.

2. *Authenticated Acknowledgement scheme:*

Authenticated Acknowledgement scheme defines the direction in which the data packet and acknowledgement move. Let N1, N2, N3 are the nodes participating in the network. They are the route chosen by the source node to transfer the data packet. The node N1 is the source node and the let the destination node be N3. The node N1 sends the data packet to nodeN2 and the node N2 forwards the data packet to node N3. The destination node N3 has received the data packet but the source node is unaware of it in the Disruption Tolerant Network. Now the authenticated acknowledgement along with the ID of the data packet is sent by the node N3 to node N1 confirming that the data packet had reached the destination. The triplet [N1 N2 N3] is formed where the node N1 acts as the monitor which monitors N2 and N3.N1 is termed as the acknowledgement receiver and N3 is termed as the acknowledgement sender.

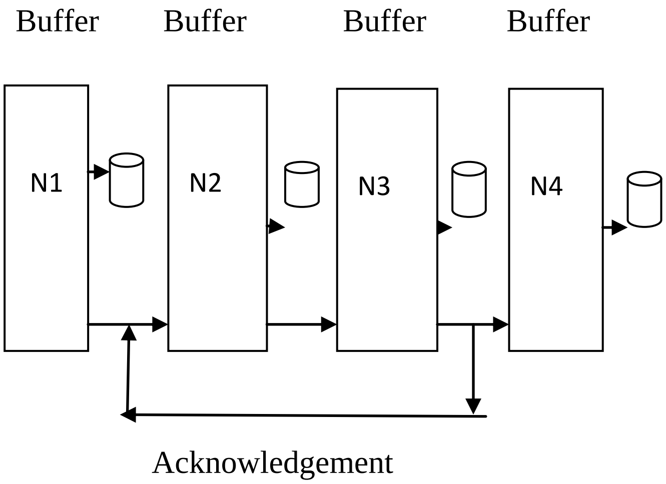


**Fig 2:** Data packet and acknowledgement direction

**Data packet Authentication:**

The acknowledgement packets are sent through the intermediate nodes, the intermediate nodes may behave selfish by not forwarding the packets. They may behave as normal nodes and provide false acknowledgement to the sender node. Hence it is required to protect the acknowledgment packets from selfish nodes. Each data packet is assigned with the current password. One way/one time hash function is used in the present data transfer.

### Data packet integrity:

A node when in communication with another nose, a serial line is formed by sending and receiving data packets and thereby the integrity of the packet is ensured.

### Data packet Confidentiality:

In one way/one time hash function, each time the current password is generated for each packet with current tag, current data, next data and current password.

### Algorithm of Cat Swarm Optimization Scheme:

Step 1: Record the authenticated element that has received from node N3.

Step 2: Start the observation process at randomly selected time.

Step 3: The LIST is initialized that contains data Ids, counter for forwarded packets and the counter for acknowledgement packets, counter for missing acknowledgement.

Step 4: When the data packet is forwarded then add the data ID to the LIST, Increase the counter of forwarded packets timer is recorded.

Step 5: Check the validity of authenticated element.

Step 6: When the acknowledgement packet is received then availability of data ID is checked

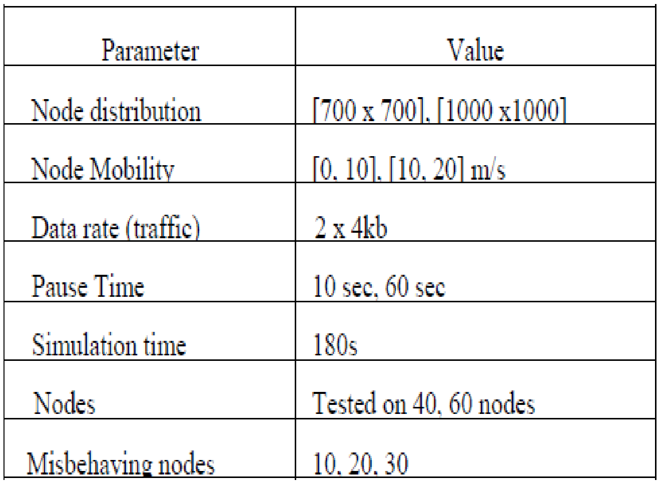
Step 7: Remove the Data ID from the LIST and clear the timer.

Step 8: When the data packet ID is not received, then remove the ID from the LIST and increase the counter of misbehaviour.

Step 9: If the period of observation expires, send misbehaviour report.

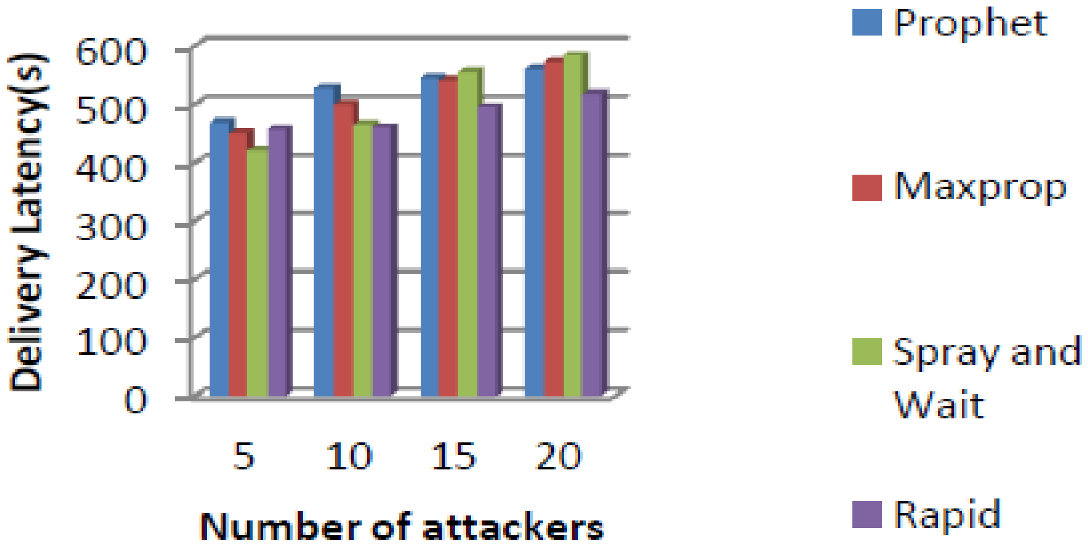
Step 10: Repeat the process for all the data packets.

### Parameters and value:



| Parameter | Value |
|---|---|
| Node distribution | [700 x 700], [1000 x1000] |
| Node Mobility | [0, 10], [10, 20] m/s |
| Data rate (traffic) | 2 x 4kb |
| Pause Time | 10 sec, 60 sec |
| Simulation time | 180s |
| Nodes | Tested on 40, 60 nodes |
| Misbehaving nodes | 10, 20, 30 |

**Packet dropping and time delay reduction:**



## CONCLUSION

As the Disruption Tolerant Networks have inconsistent connectivity between the nodes, the probability of packet dropping and time delay increases. The Cat Swarm Optimization Algorithm prevents packet dropping in DTN and thereby reducing the time delay in the network. In Cat Swarm Optimization Algorithm the authenticated acknowledgement scheme helps us to find out the selfish nodes with high accuracy, high detection rate and low false positive rate. The packet delivery ratio increases by using CSO Algorithm. The triplet form of acknowledgement ensures the authentication, integrity, confidentiality and privacy of the data packet that has been forwarded in the network. The routing misbehaviour is reduced by the direct transformation of acknowledgement from the destination node to the source node without the use of intermittent nodes. In future work, the Cat Swarm Optimization scheme can be used in different types of network to detect various types of attacks.

## REFERENCES

[1] **Thi Ngoc Diep Pham and Chai Kiat Yeo, (2016)** "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1116-1129, May 2016.

[2] **M. Chuah, P. Yang, and J. Han, (2007)** "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in In Proceeding 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Computing, 2007, pp. 1-8.

[3] **F. Li, J. Wu,and A. Srinivasan, (2009)** "Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," In Proceeding INFOCOMM, pp. 2428–2436, 2009.

[4] **Y. Ren, M. Chuah, J. Yang, and Y. Chen**, **(2010)** "MUTON: Detecting malicious nodes in disrupt-tolerant networks," inin Proceeding IEEE Wireless Communication Networking Conference, 2010, pp. 1-6.

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

[6] **Y. Guo, S. Schildt, and L. Wolf, (2013)** "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.

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

[8] **Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, (2014)** "PMDS: A probabilistic misbehaviour detection scheme toward efficient trust establishment in Delay-tolerant networks," IEEE Transaction on Parallel and Distributed System, vol. 25, no. 1, pp. 22-32, Jan 2014.

[9] **Mythili M. and Renuka K., (2016)** "An Efficient Black Hole and Gray Hole Detection Using Fuzzy Probabilistic Detection Scheme in DTN," International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 10, pp. 123-127, October 2016.

[10] **A. Keranen, J. Ott, and T. Karkkainen, (2009)** "The one simulator for dtn protocol evaluation," in Proc. 2nd Int. Conf. Simul. Tools Tech., Rome, Italy, March 2009.

[11] **Thi Ngoc Diep Pham and and Chai Kiat Yeo. (2016,** May) Detecting Colluding Blackhole and Greyhole attacks in Delay Tolerant Networks. ACM Digital Library.

[12] **Chaudhari Rajashri. M,Patil Manesh.P. (2017)** Performance Evaluation of Attack Detection Algorithms in Delay Tolerant Networks International Journal of Computer Applications (0975 –8887) Volume171 –No.4, August 2017.

[13] **AtulSharma et al, (2016)** Simulation of PSO using ONE Simulator in DTN, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)e-ISSN: 2278-2834, p-ISSN: 2278-8735.PP 47-51

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

[15] **Premanand, R.P., Rajaram, A**. Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET. Peer-to-Peer Netw. Appl. 13, 2089–2098 (2020). https://doi.org/10.1007/s12083-019-00824-1