Trust Based Node Recovery and Checkpointing Techniques in Manets

Rupali Mittal
M.Tech Research Scholar
Department of Computer Engineering
Punjabi University, Patiala, India
mittal.rupali27@gmail.com

Dr. Jaswinder Singh
Assistant Professor
Department of Computer Engineering
Punjabi University, Patiala, India
jaswindersinghmtech@gmail.com

Abstract*:* Checkpointing is a process of determining the vulnerability of node in case of any attack occurs in the network. It depends on the cluster change count value of the node. If the measure of the hop exchanges required to reach the destination node from the current node, is above the previously specified value, the node under consideration is unsafe and safe points must be implemented in between the path and different subnetworks within that network must have their own implemented safe points. The message must commits to the safe points as it reaches the respective sub networks.

The message in the networks evolve over the certain subnetworks. The each subnetwork has the checkpoint node, that serves the purpose for communication between different subnetworks, or between the hops in different subnetworks. This phenomenon supports the system efficiency and preserves the robustness. The process retrieval methods, therefore, should be implemented with the use of the safe points to prevent system degradation. In this research paper, an efficient recovery protocol is designed for distributed transactions in MANETs so that failures can be minimised. Dynamic analysis has also been done and it is compared with other existing protocols to validate the attained result.

Keywords: *Manet*

*****

I. INTRODUCTION

A MANET is self- configuring network connected without links. The nodes that have to participate in MANETS do not need any extraneous knowledge about the network parameters before joining the network. In mobile ad-hoc network, every mobile node is free to move in any direction and will therefore transform its links to other devices repeatedly. The main objective in creating a MANET network is to retain the information required to properly route the traffic. They have one or numerous and dissimilar transceivers between nodes. This results in a highly dynamic, autonomous topology. Distributed systems nowadays are used in each and every field and provide many applications like Client-Server systems, transaction processing, World Wide Web and many more. When these systems are exposed to attacks and their computation of recovery become a huge problem. Hence, various methodologies have been presented to enhance their reliability and reduce the risk of failures that involve rollback recovery, transaction and group communication.

The retrieval by pushing back all the updates, view the system as the batch of tasks transmitted over the local area networks. The various actions involved refers to a large static database which provides more robustness to the system and prevents the system degradation. If the update received is the deferred or partial update, that is, the update has not been made completely, then the process will return or retrieved back to its initial stage, referring to the static database, which has the initial information stored for all the processes involved by the system. Hence, protects the process to go out of state. For the purpose, the database push all the partial updates and recover the process to the previous saved point defined in the database. The 'undo' and 'redo' operations are applied to the processes. In case of deferred updates, if the process has committed to some checkpoint, then the redo operation is implemented on the aborted process. If the process aborts before committing to any safe point then the process is undone and all the updates made are withdrawn and process is moved to its initial state. The process retrieval operations or techniques i.e. the log-based recovery protocol or the two-phase commit protocol necessitate some extra details to be added for the operation to be done. The rollback recovery technique also imposes certain disadvantages. This technique implement various safe points in between the initial state and the final state. Is some process in execution has not committed to any of the safe points, and gets terminated, then all of its updates will be undone and process needs to be executed from the crash. Other issue is that, the system has to maintain the large database to keep track of the updates that have been done for the various processes. When the process gets aborted after committing to specific safe point, then redo operation is applied and system needs to keep track of the updates which needs to be recovered after the process is re-executed**.** When the particular process gets aborted, then effect propagates to some other processes in the system. The process having their execution connected to that specific process, also terminate their execution or needs to be re-executed.The process recovery techniques based on the use of various safe points between the initial and final points requires empty space or the database to store the updates related information. As more and more transaction updates are being made by the process in execution, the overhead of the system sometimes increases in order to maintain the record of all the updates. Also when the process aborts in between the two checkpoints, then the system needs to decide, which updates needs to be preserved and which need not to be. The updates which are not made completely or are partial, required to be removed when the process re-executes. Hence, to keep track of all the things, the automatic memory management techniques need to be implemented to serve the purpose. The rollback based recovery techniques is being used in many real-time based applications. The advantages of this technique includes the applicability of the robustness for the system. In case of certain process gets aborted in between two checkpoints or the process has committed some safe point, then all the updates that have been done after the previously committed safepoint/checkpoint need to redone. The process need not to be executed from the crash. The rollback process recovery protocol is basically of two types. One with the uncoordinated safepoints and other with the coordinated safepoints. In case of technique with coordinated safepoints, the various safepoints between the initial and the terminated state are defined in the start before the execution of the process. The process after undergoing the specified update criteria, commits to the next safe point from the present state and updates made till that point are preserved for the future. In the other technique with the uncoordinated safepoints, the process can create the safe point at the run time when required. The disadvantage of the uncoordinated safepoints is the creation of the inappropriate safepoints with the impotent updates that leads to the system overhead due to utilization of excessive resources. The technique with the coordinated safepoints has the minus point that if the process has not committed to any checkpoint before it gets aborted, the process needs to be re-executed from the starting of time, this phenomenon is called as domino effect. The process in this case has to secure the minimum required updates to achieve the stable state. Hence, the rollback technique with the coordinated and uncoordinated checkpoints is well grounded but impose few restrictions. The rollback technique for the process recovery is recommended for the systems with the large resources available to maintain a database in order to keep track/record of the updates made by the several processes in execution. Also this technique requires the replications of the same data to be stored at the different locations to store different purposes. These includes, retrieving the process back to the particular pre-final state, to decide which of the updates made by the process need to be retained when it gets aborted.

II. RELATED WORK

Neeraj Sharma and Ravneet Kaur[2015] in this paper Dynamic Node Recovery approach have been presented. This approach is employed genetic algorithmic operations to ensure optimal recovery of checkpoints in case of node failures. Refinement of some of the aspects of the existing base approach reduces the recovery time considerably, thereby, improving the throughput of the network. It also enhances the network lifetime as the proposed approach leads to lower energy level drops in the nodes.

Poonam Saini and Shefali Aggarwal[2015] presented Coordinated and Uncoordinated Check pointing in MANET. The proposed checking point approach is based on movement of node. In this paper various techniques based on rollback recovery have been discussed. Additionally, a multi-check pointing protocol has been proposed which reduces overall overhead incurred while check pointing.

Tuli Kumar and P.K Jaggi[2013] discussed the technique for the wireless communication networks, where the communication is generally carried between the two or more hosts on different networks. The safe points or the check points are defined for the processes within those systems, which are geographically distributed over the large clustering regions. The safe points are defined between the different hosts/nodes for communicating the message. If the process/message has been committed to certain safe point, then the information is updated at the dedicated database for the purpose located at the base station. If the certain host network not able to communicate the message to the intended receiver network, followed by the failure to commit to the safe point, then the message is retrieved back to the pre-final or the initial state. In this case, the redo operation is carried out and the message is re-transmitted using different host network. The process is called the hand-over and the checkpoints used here are process non-blocking checkpoints.

Doug Hakkarinen and Zizhong Chen [2013] defined the technique in which the numerous checkpoints are defined. The process based on the updates made by its execution, commits to or assigned to the particular checkpoint. If some safe point or the checkpoint is never been assigned to any process in execution then it is of no use. Hence, need to be removed from the system database to free some space to be utilized for the other purposes. To serve the purpose, the process needs to keep track/record of various checkpoints. This technique also minimize the overhead to the system as the inappropriate checkpoints are deleted from the database. This technique of the process recovery based on checkpoints provided better results when compared with the existing techniques. The technique is utilized for the wireless mobile ad-hoc networks**.**

Jaggi Singh and A.K [2011] proposed algorithm by using Self Stabilizing Tree. The person behind this research work described an algorithm for recording steady global picture of dynamic MANET network. In order to minimize the snapshot related message as spanning tree, all other cluster heads systematize themselves into a self stabilizing spanning tree. The result from tree will always provide result in shortest possible path. The result indicates that if number of cluster is increased the number of control message decreased significantly. Furthermore, it can be concluded that proposed algorithm may efficiently works with multiple initiators and dynamic topology.

A.K .Singh and P. K. Jaggi [2011] discussed a technique in which the process itself needs to act jointly with the checkpoints. The various checkpoints are stored in the database, the process needs to commit certain safepoint based on the updates made by the execution of the process. In this case, the process is not stick to the phenomenon that it needs to commit to the first received checkpoint, as in the case where the checkpoints are statically defined between the initial and final points. Here the criteria is followed, where the updates are made by the process and based on the updates the safe point or pre-final state is achieved dynamically. This type of techniques helps the system to cope up with the failures more efficiently, and the aborted process can be easily retrieved to its pre-final state. Overhead of the system also get minimized. This technique is particularly designed for the mobile ad-hoc networks.

Suparna Biswas et. al. [2011] discussed the rollback process recovery technique and checkpoints for the mobile ad-hoc networks. In this technique the sending mobile hosts communicate the message with the two or more receiver hosts. The safe points are defined on the networks between the sender host and the various receiver hosts. When the process/message commit to some safe point on the particular host to host or node to node network line, then the update/record is made to the database/routing table of that particular receiving host/node. The system is highly efficient as if the message can't be transmitted over one network, it is diverted to some other network with less traffic or overhead based on the information stored in the routing tables of the receiving nodes.

Qiangfeng Jiyang et al. [2008] discussed the process retrieval technique based on the offline processing of the incoming and outgoing messages for the systems located at the different geographic locations. This technique basically implements system in which the process itself creates the checkpoints depending upon the requirement. This technique prevents the inefficient utilization of the system resources. The message is sufficiently processed for making the required updates and then it is committed for the next safe point and all the updates made are recorded to the dedicated database maintained for the purpose by the various systems at different locations. This technique is effective and prevents the system degradation**.**

Tong- Tony –Chang et al. [2007] discussed a new solution to crash recovery. Processor will start from its most current saved state in case of any failure. The result indicates improved result compared to existing approach.

Masakazu Ono and Hiroaki Higaki et al. [2007] presented a checking point approach by using flooding method. In this scheme, mobile host can able to communicate without enough bandwidth and stable approach. By using flooding method, checkingpoint request is being sent each mobile host of a node save the information of a node. In case, when any node suffers from any lost information and then this lost message/information is stored by its intermediate nodes.

Table 1: Comparison table

S.NO.	NAME OF THE AUTHOR	APPROACH USED	CONCLUSION
1.	Neeraj Sharma and Ravneet kaur [2015]	Dynamic Node Recovery approach	Enhances the network lifetime
2.	Tuli Kumar and P K Jaggi. [2013]	The minimum number of nodes that the process needs to travel before committing the first safe point in the subnetwork.	Reduces the energy consumption and recovery latency
S.NO.	**NAME OF THE AUTHOR**	**APPROACH USED**	**CONCLUSION**
3.	Hakkarinen Doug and Zizhong Chen [2013]	Multilevel diskless checkpointing approach	This method improves expected execution time
4.	Suparna Biswas, Priyanka Dey et al. [2013]	A hybrid model of secure checkpointing	The efficiency of the system improves, the minimum number of the hopes that the process needs to travel for committing safe point reduces
5.	A. K .Singh and P. K. Jaggi [2011]	Manually creates the check points in the system, where the process has the probability to get failed	Increase he robustness of the system by reducing the multiple failures in the system.
6.	Jaggi singh and A.K. [2011]	The process updates routing tables of all the nodes in the subnetwork when the process commits to the safe point defined by the specific subnetwork	Efficient approach, decreasing the number of control messages
7.	Suparna Biswas et. al, [2011]	Mobility based checkpointing approach and trust based rollback recovery	The process retrieval is affordable and the ensures the system robustness, prevents system degradation
8.	Jiyang Qiangfeng et al. [2008]	The process retrieval and the message recovery process using safe points within the system	Improved result and Minimize the network contention

9.	Tong- Tony –Chang et al. [2007]	Rollback recovery approach in conjunction with checkpointing	Improved result compared to existing approach.
10.	Masakazu Ono, Hiroaki Higaki et al. [2007]	Checkingpoint approach by using flooding method.	Improving throughput of network

III. PROPOSED METHOD

This paper proposes a novel method of checkpointing based on trust value of nodes in MANET. confidence value of a process depends on the subnetwork in which the process lies at the specified time, the number of checkpoints committed by process moving from the current node to the destination node, and the predefined required value of the confidence.

Confidence value of the network depends upon the count of processes in the network having the confidence value higher than the predefined, specified value i.e. threshold.

$$Confidence\ value\ of\ process\ in\ network = \frac{\sum Checkpoints\ committed\ by\ the\ process}{number\ of\ checkpoints\ in\ the\ network}$$

The confidence of the process is the proportion of the safe points committed by the process to the total safe points in the whole network. Where, each subnetwork has its own defined safe point.

The value of the confidence is calculated in the equation above specified. The confidence value is basically the proportion of the safe points that have been committed by the process to the total safe points in the network. Where, each subnetwork has its associated check point. The summated average of confidence values for the processes in subnetworks signifies the confidence of whole subnetwork. The measure of confidence of the various subnetworks in network supports the efficiency of the whole system. If the process with the higher confidence value moves within the networks then the overall system 'support' increases. When some process is found to be unsafe then that process committed to the first safe point between the source and destination. The routing table of the hop associated with the committed safe point within the subnetwork is updated. When the process moves from the source to destination hop within the network, to find the optimum path, we must keep in track the safe points to which the processes have committed for the most. When the process has committed some safe point, it should be routed towards the another safe point(in different subnetwork), which has been mostly committed by the system processes. The whole criteria is followed in the recursive manner, the operation is applied for the different safe points in the different subnetworks, until we obtain the feasible solution.

A. PSEUDO CODE

```
$Start$
$Initialize\ the\ node\ parameters\ and\ trust\ value$
$Calculation\ of\ Initial\ Cluster\ trust$
$for\ i\ in\ 0\ to\ n, where\ n\ is\ number\ of\ nodes$
    $t \leftarrow \frac{N_{ct} - P_{ct}}{P_{ct}}$ $, where\ t\ is\ trust\ of\ node\ and\ P_{ct}\ is\ the\ previous\ cluster\ trust\ and\ N_{ct}\ is\ the\ next\ or\ target\ cluster\ trust\ value$
    $CC \leftarrow 1 - (N_{ct} - P_{ct})$ $, where\ CC\ is\ cluster\ cahnge\ count$
$end\ for$
$if\ CC > threshold$
    $for\ i\ in\ 0\ to\ m, where\ m\ is\ number\ of\ vulnerable\ nodes$
        $Calc\ (m_s, m_d), calculation\ using\ som\ algorithm$
        $m_s\ is\ recovery\ node\ and\ m_d is\ checkpointing\ node$
    $end\ for$
$end\ if$
$end$
```

B. Performance Parameters

1: Recovery Probability: Node recovery after failure is defined as the probability of recovery. It depends on the trust value of the node which needs to be recovered and cluster change count.

2: Residual Energy: The energy remaining at each node after the transmission and reception cycle is termed as residual energy of the node. It is directly related to the network lifetime of the node.

IV. RESULT AND DISCUSSION

In figure 1– 2 residual energy is compared with respect to the simulation time for different number of nodes i.e. 50 and 20 respectively and in figure 3-4 probability of recovery is compared with respect to the simulation time for different number of nodes i.e. 50 and 20 respectively. In figure 5-6 packet delivery delay is compared with respect to the simulation time for different number nodes i.e. 50 and 20 respectively and in figure 7-8 packet delivery ratios is compared with respect to the simulation time for different number of nodes i.e. 50 and 20 respectively.

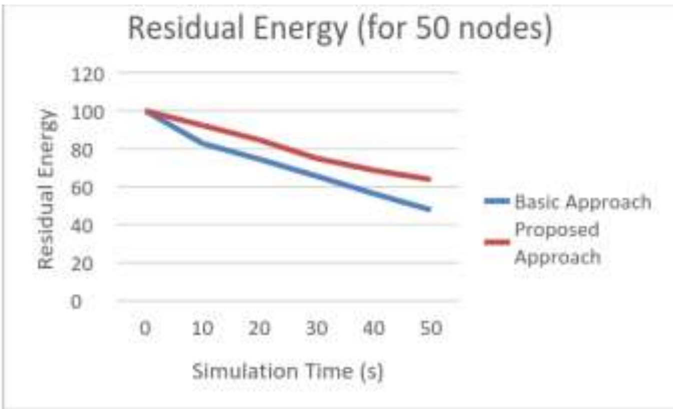

Fig 1: Residual Energy Vs Simulation Time (50 nodes)

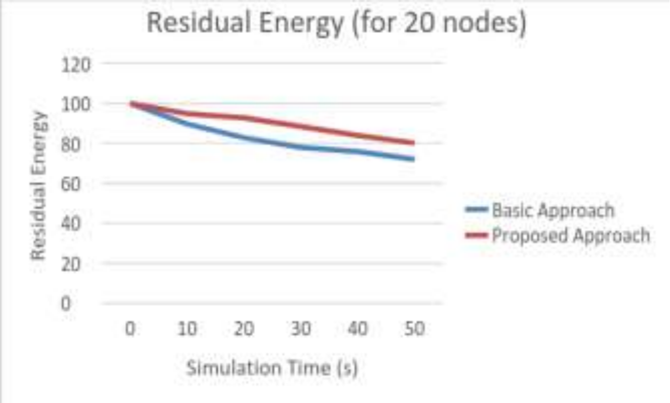

Fig 2: Residual Energy vs Simulation Time (20 nodes)

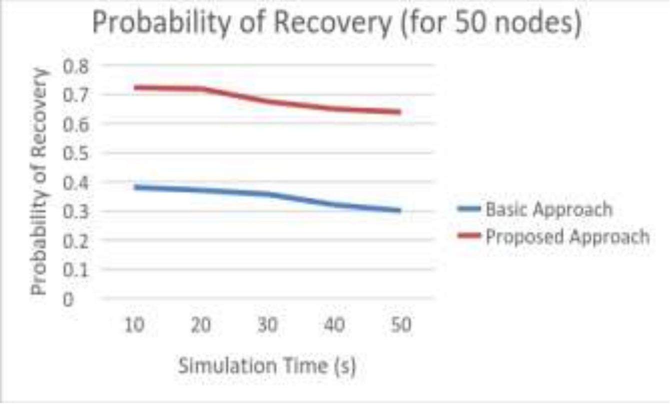

Fig 3: Probability of Recovery vs Simulation Time (50 nodes)

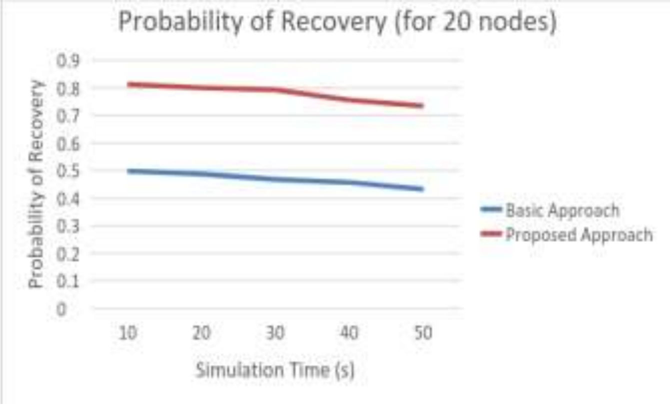

Fig 4: Probability of Recovery vs Simulation Time (20 nodes)

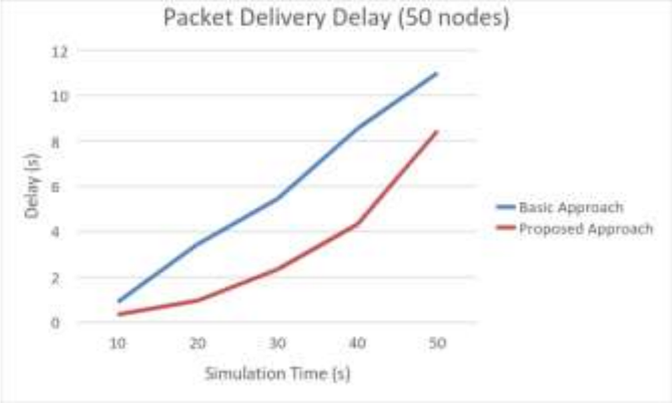

Fig 5: Packet Delivery Delay vs Simulation Time (50 nodes)

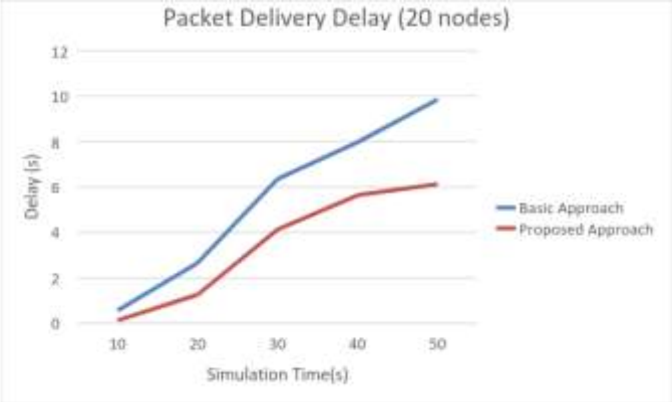

Fig 6: Packet Delivery Delay vs Simulation Time (20 nodes)

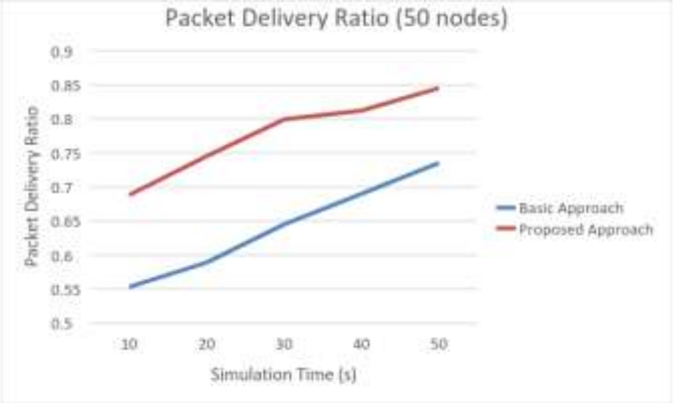

Fig 7: Packet Delivery Ratio vs Simulation Time (50 nodes)

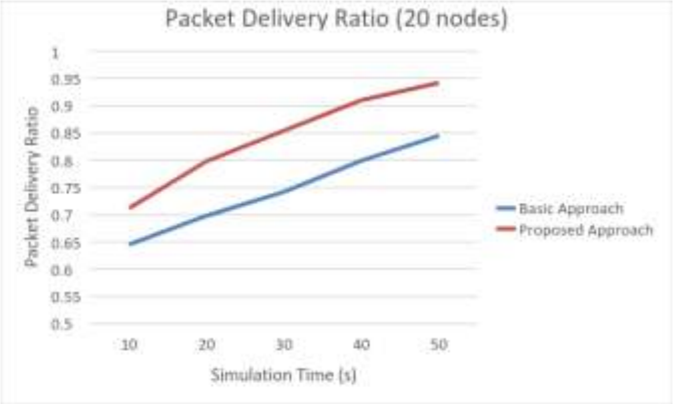

Fig 8: Packet Delivery Ratio vs Simulation Time (20 nodes)

V. CONCLUSION

The mechanism of network node recovery is a topic of concern and new techniques have been evaluated along with the existing ones. Various checkpointing and node recovery techniques are compared in the present work and their performance on various parameters like packet delivery ratio, throughput of the network. The nodes present in the network are likely to be attacked and save their checkpointing data to the host cluster head. A node in mobile environment can pass through diverse clusters in its lifetime towards various attacks. The secure route selection in the network must solve this purpose of increasing overheads. The selection of the recovery node and the checkpointing node must also be selected in terms of the available resources on them. In the methodology proposed, the trust is increased according to the opinion dynamics rule. Another important aspect is to find out the better combination of both the algorithms (Firefly and GA). So these aspects must be covered in the future scope and can be compared with the existing results of our algorithm. This work has also concluded that MANET has to handle number of issues like stable storage, battery consumption, different overheads, topological changes and traffic load with the clusters. Moreover, we propose a multi-checkpointing movement based trust model for checkpointing which reduces overall overhead incurred while checkpointing.

REFERENCES

1. A. K. Singh and P. K. Jaggi, "Staggered checkpointing and recovery in cluster based mobile ad hoc networks." *Advances in Parallel Distributed Computing*, pp 122-134, 2011.
2. Chih-Cheng Tseng and Kwang-Cheng Chen, "Organizing an optimal cluster-based ad hoc network architecture by the modified quine-mccluskey algorithm." *IEEE Communications Letters*, Volume 11, Issue 1, January 2007.
3. Doug Hakkarinen and Z.C, "Multilevel diskless checkpointing." *IEEE Transactions on Computers*, Volume 62, Issue 4, pp 772-783, April 2013.
4. Masakazu Ono and H.H, "Consistent Checkpoint Protocol for Wireless Ad-hoc Networks." In *PDPTA*, pp 1041-1046, 2007.
5. P.K Jaggi and A.K , "Message efficient global snapshot recording using a self stabilizing spanning tree in a MANET." *International Journal of Communication Networks and Information Security*, Volume 3, Issue 3 , pp 247, December 2011
6. Qiangfeng Jiang, Yi Luo, and D. Manivannan, "An optimistic checkpointing and message logging approach for consistent global checkpoint collection in distributed systems." *Journal of Parallel and Distributed Computing*, Volume 68, Issue 12 , pp 1575-1589, December 2008.
7. Ravneet Kaur and Neeraj Sharma, "Dynamic node recovery for improved throughput in MANET." In *1st International Conference on Next Generation Computing Technologies (NGCT)*, pp 325-330, IEEE, September 2015.
8. R Tuli and P.K , "Minimum process coordinated Checkpointing scheme for ad hoc Networks." *International Journal on AdHoc Networking Systems (IJANS)*, Vol. 1, No. 2 ,pp 51-63,November 2013.
9. Shefali Aggarwal and Poonam Saini, "Coordinated and uncoordinated checkpointing in mobile ad hoc networks." In *2015 International Conference on Computing, Communication & Automation (ICCCA)*, pp 611-615, IEEE, May 2015.
10. Suparna Biswas, S. N "A Handoff based Checkpointing and Failure Recovery Scheme in Mobile Computing." *International Conference on Information Networking*, September 2011.
11. Suparna Biswas, Priyanka Dey and Sarmistha Neogy, "Secure checkpointing-recovery using trusted nodes in MANET. "In *4th International Conference on Computer and Communication Technology (ICCCT)*, pp 174-180, IEEE, September 2013.
12. Taesoon Park and H.Y, "An asynchronous recovery scheme based on optimistic message logging for mobile computing systems." In *Proceedings. 20th International Conference on Distributed Computing Systems*, pp 436-443, IEEE, 2000.