Secure Check-pointing and Recovery in Mobile Ad Hoc Network

Sandeep Dhiman[1], Amandeep Singh[2]
[1]M.Tech Scholar, [2]Associate Professor
Rayat Institute of Engineering and Information Technology, Ropar, India

***Abstract* -** In this thesis an efficient recovery protocol is designed for distributed transactions in MANETs that ensures secure transfer of checkpoints of mobile hosts in case of node failures while keeping in consideration several factors such as mobility pattern of the nodes, security attack rate, battery power of the nodes and human opinion dynamics. The proposed protocol also used to recover from failures that need to be minimized. This will improve the performance parameters of the cluster-based ad hoc network including throughput, energy utilization, secure communication etc. Dynamic analysis has also been done and it is being compared with other existing protocol to validate the attained result.

Keywords - MANET

I. INTRODUCTION

A MANET is self- configuring network connected without wires. With the creation of mobile devices (cell phones, personal digital PDA, laptops, and other handheld digital devices), and the exponential growth in the wireless sector in the past decade, there is a revolutionary change in the way information is being handled. In mobile ad-hoc network, every mobile node is freely moved in any direction and would therefore transform its links to other devices repeatedly. The prime objective in creating a MANET network is to sustain the information required to properly route traffic. They may have one or numerous and dissimilar transceivers between nodes. This results in a highly dynamic, autonomous topology. Distributed systems nowadays are everywhere and facilitate many applications like Client-Server systems, transaction processing, World Wide Web and many more [2]. The huge computing possibility of these systems is often hindered by their exposure to failures. Hence, numerous approaches have been presented to enhance the reliability and reduce the risk of failure that incorporates rollback recovery, transaction and group communication.

Rollback recovery treats processes having right to use to a stable storage area that survives a variety of kinds of failures. These processes can tolerate failure by saving their recovery information on these storage devices. If failure occurs than these processes recover by using this saved information from these devices. This recovery information contains at least the states of these processes called *check points.* Other recovery protocols other than rollback recovery also require other additional information. Rollback recovery can have different essence like it may require an application to decide when and what to save. If failure occurs in any process then these dependencies may force a number of processes to rollback leading to a problem called *rollback propagation.* Under some cases rollback propagation may widen back to the initial state of computation leading to the failure of all the computation done yet. This condition is called *domino effect.*

Checkpointing algorithms put away abundance of resources. As the calculation remains growing and total information collected increases, though after some time the majority of this information is of no use. Consequently, in order to free this space, garbage collection is done in which of deletion of this useless information to free this space. In mobile computing, checking point is one of the significant fault tolerant approaches. Present status of information has been recorded that can be required during the recovery after failures. Therefore, calculation can be restarted from point of saved checkpoint in case of failure rather from beginning. The proposed approach. Check pointing-based rollback recovery is used in various domains like, database management, applied sciences computer networks and many more. There is various numbers of protocol which is useful but those protocol which is based on checking point are very easy to implement and having very few limitations. Therefore, protocol is not responsible for the system is roll backed to pre failure state. Hence, it can be concluded that system based on checking point rollback recovery is appropriate for those system that are in continuous communication with external world.

Uncoordinated checkpointing provide every practice a freedom to obtain checkpoint anytime devoid of any constraint or limitation. Hence, a method could obtain checkpoint at whatever time. Moreover, uncoordinated checkpointing have some issues which lead to failure of all stored information or data. This issue referred as domino effect. One another issue which may leads to taking of useless checkpoints that enhances the wastage of space. In Coordinated checkpointing the processes needs to coordinate with their checkpoints to arrive at a reliable state. General technique is utilized to increase the probability of the data which is being sending to imitate several copies of data in the hope that it will definitely achieve its destination. It is only possible on the network having large amount of local storage with respect to expected traffic. It is in the context of the last two issues that checkpointing and rollback recovery comes into picture. Recovery techniques processes have access to a steady storage area that survives various types of failures. These processes can tolerate failure by saving their recovery information on these storage devices.

II. RELATED WORK

QiangfengJiyang et al, [1] presented a message logging approach in distributed systems. This proposed approach is based an optimistic checkpointing. Each and every message which is sent and received is stored after tentative checkpoint. This method took enough time to take checkpoint and hence it is capable of reducing the network contention. The result indicates that proposed approach is very reliable and efficient.

A. K .Singh-P. K. Jaggi et al. [2] discussed the coordinated checkpointing scheme. In this approach self-stabilizing spanning tree are utilized leading to the network topology to minimize the overhead issue and on the other hand it deals with dynamic properties of MANET. To evade the concurrent resources, staggered checkpointing approach has been presented in this paper. This proposed protocol does not require any FIFO channel. The proposed protocol helps to maintain the initiation of concurrent checkpoint and also it successfully deals with overlapping failures in MANET.

Jaggi-Singh et al. [3] 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.

Tuli-kumar et al. [4] in this paper, non-blocking and minimum process checkpointing scheme have been discussed for clustering protocols. This scheme fulfills the requirement of ad-hoc environment. In this approach, all the information related to cluster head is stored in the base station. When cluster head required sending routing then other nodes collected the information to it. In case when cluster head is failed then some other mobile host is assigning to it complete the task of cluster head. Hence it can be said that proposed approach minimizes the energy consumption and recovery latency.

Suparna Biswas et. al, [5] proposed a mobility based checkpointing and trust based rollback recovery for fault-tolerance in MANETs. In MANET, every mobile node is freely moved in any direction and would therefore transform its links to other devices repeatedly. The main aim in creating a MANET network is to sustain the information required to properly route traffic. The proposed approach resulted in low recovery cost and high recovery probability of failed mobile hosts.

Doug Hakkarinen and Zizhong Chen et al. [6] proposed a multilevel diskless checkpointing. This proposed approach is needed to find the optimal checkpoints and number of level which gives valid starting point. The result indicates that N-level diskless checkpointing is highly capable system. The experimental Results conclude that presented scheme provides high performance computing programs as compared to previous systems. Moreover, this approach enhances the expected execution time especially in case large number of process required.

Suparna Biswas and Priyanka Dey et al. [7] proposed a secure checkpointing recovery using trusted nodes in MANETs.They may have one or numerous and dissimilar transceivers between nodes. Additionaly, hybrid model of secure checkpointing in which proposed trust model is mutual with encryption scheme.This results in a highly dynamic, autonomous topology and therefore increases applicability of this model in MANET environment with least resources.

Tong- Tony –Chang et al. [8] 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. [9] 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.

Neeraj, Ravneet et al. [10] 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, Shefali Aggarwal et al. [11] 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.

Table 1: Comparison table

S.NO	NAME OF THE AUTHOR	APPROACH USED	CONCLUSION
1.	Qiangfeng Jiyang et al. [1]	An optimistic checkpointing and message logging approach	Improved result and Minimize the network contention
2.	A. K .Singh-P. K. Jaggi, et al. [2]	A coordinated checkpointing scheme, staggered checkpointing approach	Successfully handles the overlapping failures in MANET
3.	Jaggi singh et al. [3]	A Snapshot recording using a Self-Stabilizing Tree	Efficient approach, decreasing the number of control messages
4.	Tuli-kumar et al. [4]	A non-blocking and minimum process checkpointing scheme	Reduces the energy consumption and recovery latency
5.	Suparna Biswas et. al, [5]	Mobility based checkpointing approach and trust based rollback recovery	Low recovery cost and high recovery probability of failed mobile hosts.
6.	Doug Hakkarinen, Zizhong Chen et al. [6]	Multilevel diskless checkpointing approach	This method improves expected execution time
7.	Suparna Biswas, Priyanka Dey et al. [7]	A hybrid model of secure checkpointing	Energy consumption of nodes and bandwidth consumption get reduced
8.	Tong- Tony – Chang et al. [8]	Rollback recovery approach in conjunction with checkpointing	Improved result compared to existing approach.
9.	Masakazu Ono, Hiroaki Higaki et al. [9]	Checkingpoint approach by using flooding method.	Improving throughput of network
10.	Neeraj, Ravneet kaur et al. [10]	Dynamic Node Recovery approach	Enhances the network lifetime

III. PROPOSED METHOD

The thesis proposes a novel method of checkpointing based on trust value of nodes in MANET. Trust of a node is calculated which relied on the trust level of the cluster in which the node is present on a specific instant of time and the cluster alter count threshold value.

Trust value of each cluster is estimated on the basis of the number of trustworthy nodes present in the cluster.

$$\text{trust value of cluster} = \frac{\sum trust\ value\ of\ each\ node\ in\ the\ cluster}{number\ of\ nodes\ in\ the\ cluster}$$

Trust value of the cluster is referred as the ratio of the summation of trust value of each node in the cluster) to the number of nodes in the cluster. From above mentioned formula it can be concluded that trust value of the nodes is directly proportional to trust value of the cluster. There for when the trust value of the nodes in the cluster increases then trust value of cluster also increases. When node moves from one cluster to another having higher trust value, then count value is increased by very small unit and vice versa.

If a node is found to be malicious and required to be recovered then - Initially, the recovery node transfer a signal to each cluster head to locate the check-pointing node and cluster head advance forwards the signal to every nodes in the cluster. The computation of the optimal route is depending on various factors like; the optimal route carries all the trusted nodes, use less energy to transmit the data. The optimal route computation is done with the help of Self Organizing Maps algorithm that takes these factors as its weight and iteratively evaluates the optimal solution and vigorously changes its properties as per the prerequisite of the network.

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
    $t \leftarrow \frac{Nct-Pct}{Pct}$, where t is trust of node and Pct is the previous cluster trust and Nct is the next or target cluster trust value
    $C \leftarrow 1-(Nct-Pct)$, where CC is cluster change 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

(i) 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.

(ii) 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 of 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.

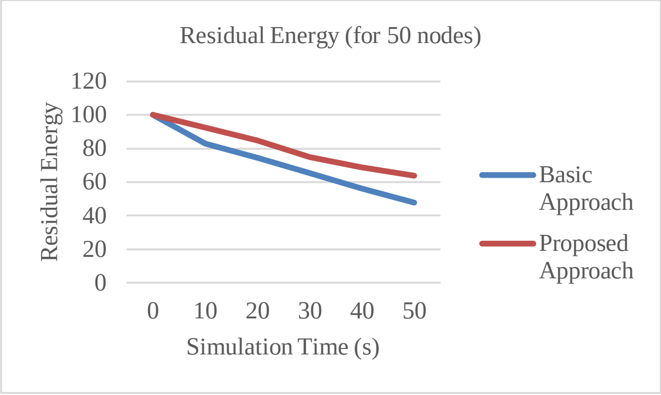

Fig 1: Residual Energy vs Simulation Time (50 nodes)

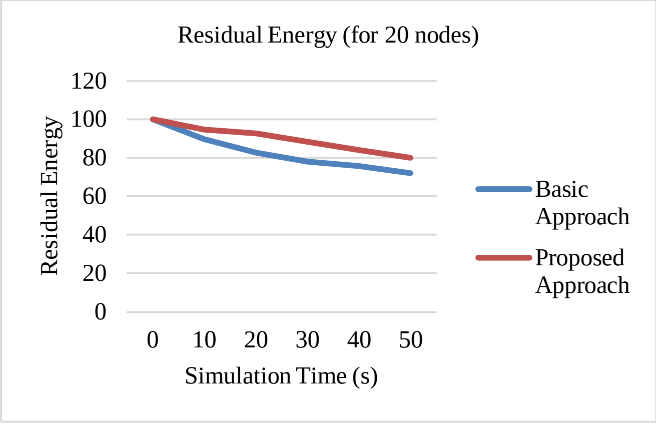

Fig 2: Residual Energy vs Simulation Time (20 nodes)

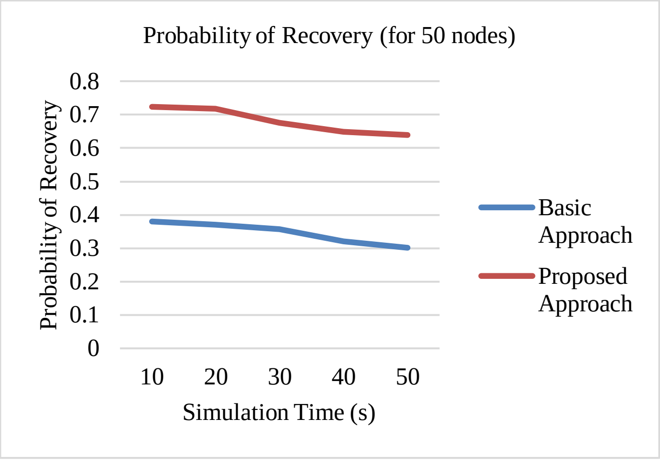

Fig 3: Probability of Recovery vs Simulation Time (50 nodes)

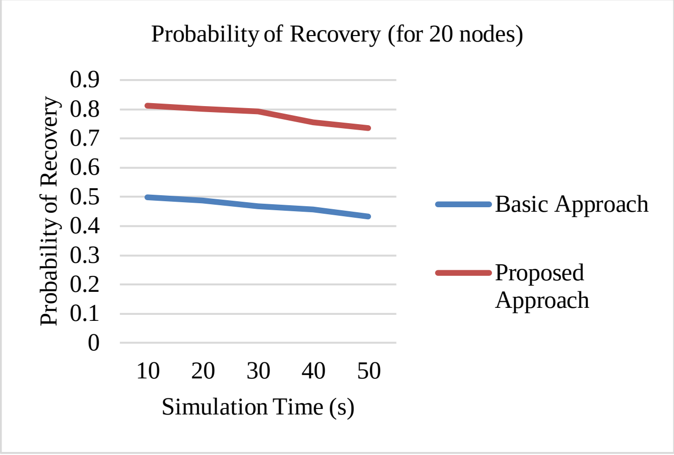

Fig 4: Probability of Recovery vs Simulation Time (20 nodes)

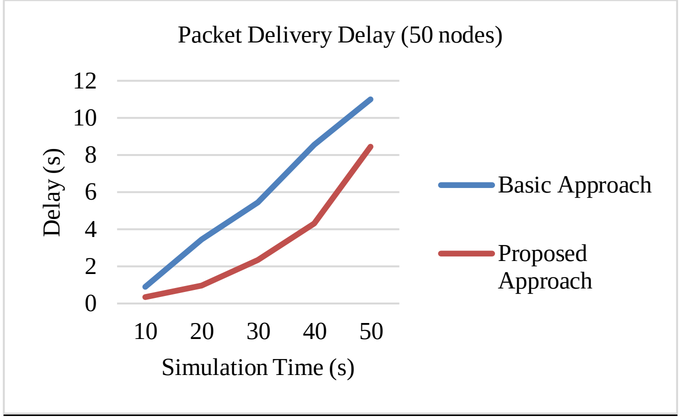

Fig 5: Packet Delivery Delay vs Simulation Time (50 nodes)

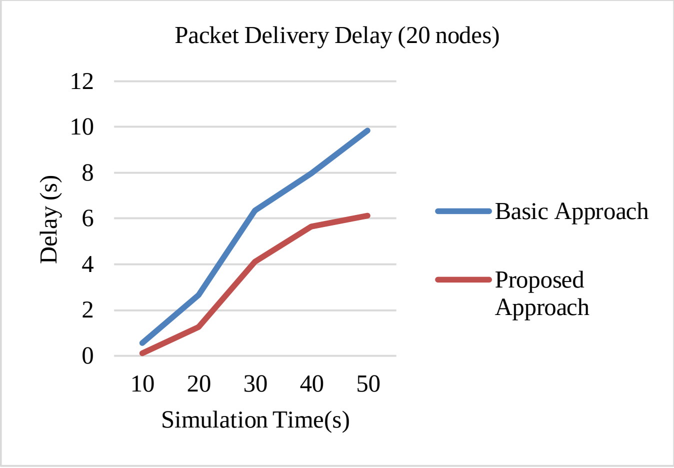

Fig 6: Packet Delivery Delay vs Simulation Time (20 nodes)

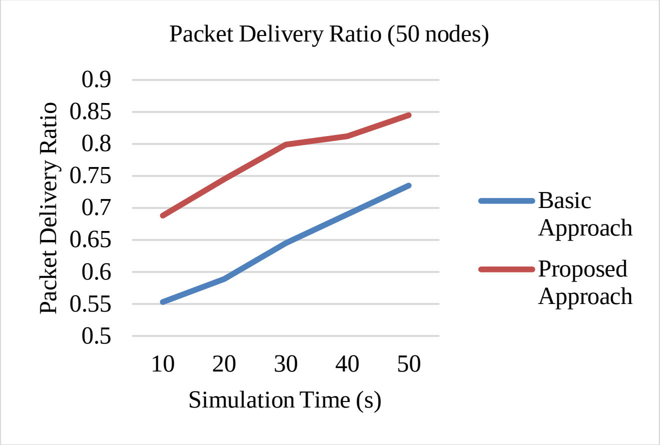

Fig 7: Packet Delivery Ratio vs Simulation Time (50 nodes)

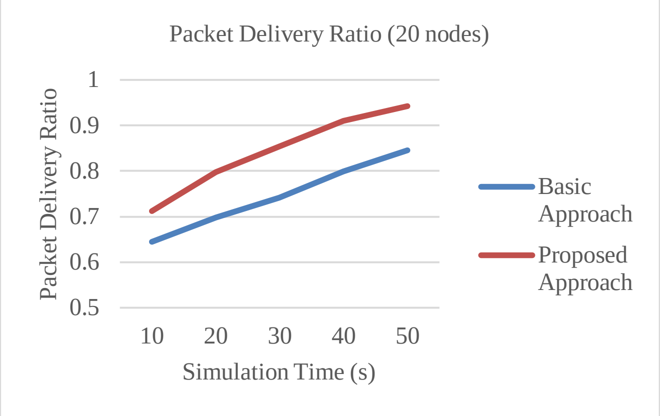

Fig 8: Packet Delivery Ratio vs Simulation Time (20 nodes)

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]. Khamrui, Pulak, and Koushik Majumder. "A trusted node based checkpointing scheme for mobile ad-hoc networks (MANETs)." In *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on*, pp. 831-836. IEEE, 2015.

[2]. Jaggi, Parmeet Kaur, and Awadhesh Kumar Singh. "Opportunistic rollback recovery in mobile ad hoc networks." In *Advance Computing Conference (IACC), 2014 IEEE International*, pp. 860-865. IEEE, 2014.

[3]. Benkaouha, Haroun, Lynda Mokdad, and Abdelkrim Abdelli. "2PACA: Two Phases Algorithm of Checkpointing for Ad hoc mobile networks." In *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*, pp. 1359-1364. IEEE, 2013.

[4]. Aggarwal, Shefali, and Dr Poonam Saini. "Checkpointing in mobile ad hoc networks (MANETs)-A survey." *International Journal of Advanced Research in Computer Science and Software Engineering* 5, no. 3 (2015).

[5]. Biswas, Suparna, Priyanka Dey, and Sarmistha Neogy. "Secure checkpointing-recovery using trusted nodes in MANET." In *Computer and Communication Technology (ICCCT), 2013 4th International Conference on*, pp. 174-180. IEEE, 2013.

[6]. Doug Hakkarinen, Z. C. (april 2013.). Multilevel Diskless Checkpointing. *IEEE transactions on computers, vol. 62, no. 4.*

[7]. Suparna Biswas, P. D. (2013). Secure Checkpointing-Recovery Using Trusted Nodes Nn MANETs. *4th International Conference on Computer and Communication Technology (ICCCT).*

[8]. Mansouri, Houssem, Nadjib Badache, Makhlouf Aliouat, and Al-Sakib Khan Pathan. "Adaptive Fault Tolerant Checkpointing Algorithm for Cluster Based Mobile Ad Hoc Networks." *Procedia Computer Science* 73 (2015): 40-47.

[9]. Jaggi, Parmeet Kaur, and Awadhesh Kumar Singh. "Rollback recovery with low overhead for fault tolerance in mobile ad hoc networks." *Journal of King Saud University-Computer and Information Sciences* 27, no. 4 (2015): 402-415.

[10]. Kumar, Parveen, and Rachit Garg. "Soft-checkpointing based hybrid synchronous checkpointing protocol for mobile distributed systems." In *Development of Distributed Systems from Design to Application and Maintenance*, pp. 87-100. IGI Global, 2013.

[11]. Kaur, Ravneet, and Neeraj Sharma. "*Dynamic node recovery for improved throughput in MANET.*" In Next Generation Computing Technologies (NGCT), 2015 1st International Conference on, pp. 325-330. IEEE, 2015.

[12]. Aggarwal, Shefali, and Poonam Saini. "*Coordinated and uncoordinated checkpointing in mobile ad hoc networks.*" In Computing, Communication & Automation (ICCCA), 2015 International Conference on, pp. 611-615. IEEE, 2015.