ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARICLE

Available Online at www.ijarcs.info

Improving Secure Check pointing Recovery Technique using Trusted Nodes

Navdeep Kaur, M.Tech. Research Scholar
Computer Engineering Department
University College Of Engineering,
Punjabi University Patiala, India
nnavdeepkaur@gmail.com

Abstract- *We propose a trust-value based uncoordinated check pointing algorithm which improves the overall check pointing overhead. Most of the check pointing approaches takes checkpoints periodically without taking into consideration the mobility rate of nodes resulting in wastage of resources and increased time delay. Our trust value based check pointing scheme allows taking check pointing only after a mobile node has made certain number of movements. The value of the cluster change count threshold when a node moves from one cluster to another cluster is dynamic, means if the number of cluster movements of a node is greater than threshold the node is said to be attack prone or unsafe to transfer secured information. A comprehensive survey of various check pointing algorithms has also been shown to gather the essential knowledge that how these algorithms work. Our proposed algorithm has three phases – multi-checkpointing phase, a trust node evaluation phase and a recovery phase.*

Keywords- *Checkpointing,Domino Effect,Recovery, MANET, Mobility.*

I. INTRODUCTION

A mobile ad hoc network (MANET) is a constantly self-configuring, infrastructure-less network of mobile nodes connected without wires. Each mobile node in a MANET is independent to move freely in any direction, and will therefore modify its links to other devices repeatedly. Each node must forward data not related to its own use. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic [1]. Such networks may operate by themselves or may be connected to the larger Internet. 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. Therefore a number of techniques have been proposed till today to increase reliability and decrease failures which include group communications, transactions, and rollback recovery.

Rollback recovery treats a distributed system as a group of processes that communicate through a wireless network. These 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. 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 or it may provide all the information itself to construct an application.

Message passing systems make rollback recovery more complicated because of their inter dependencies as shown in fig. 1. 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.

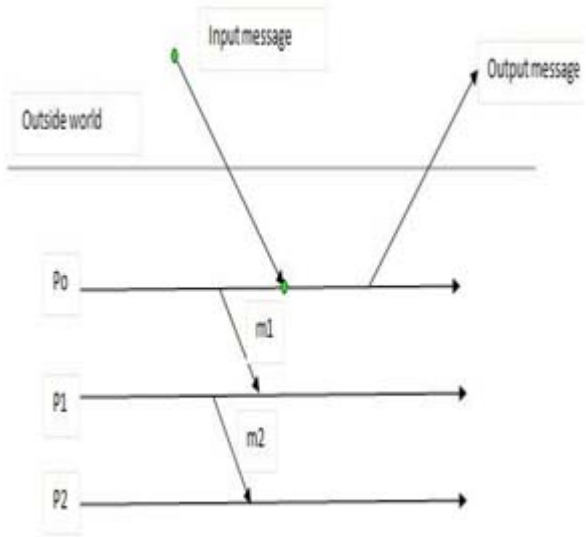

Figure 1. Message passing system

Check pointing based Rollback Recovery

In case of any failure in Distributed systems, Rollback recovery brings back the state of system to the most recent consistent state. Checkpoint based protocols are easy to

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

implement and have less restrictions. However these protocols don't ensure that the system is roll backed to pre failure state.

Therefore checkpoint based Rollback recovery is best for those systems which are in continuous communication with outside world. Checkpoint based protocols are divided into three sub categories: *Uncoordinated checkpointing, coordinated checkpointing,* and *communication induced checkpointing.*

1. **Uncoordinated Checkpointing** Uncoordinated checkpointing give each process a freedom to take checkpoint anytime without any restriction. Therefore a process can take checkpoint whenever amount of information is small. However the uncoordinated checkpointing also pose some problems like *domino effect* which leads to loss of all the saved information due to extending back to the initial computation state. Secondly, it may lead to taking of useless checkpoints which increases the wastage of space.

2. **Coordinated Checkpointing** In Coordinated checkpointing the processes needs to synchronize their checkpoints to reach a consistent state. This type of checkpointing is less prone to failure and also free from domino effect as each process initiates from its latest saved checkpoint. Moreover coordinated checkpoint ensures that each process saves its checkpoint on stable storage reducing wastage of space resulting in avoiding garbage collection. However this approach has a disadvantage of time delay due to synchronization involved.

3. **Communication Induced Checkpointing** In Communication induced checkpointing processes takes two type of checkpoints: local checkpoint and forced checkpoints. Local checkpoints can be taken independently, while forced checkpoint *must* be taken to guarantee the eventual progress of the recovery line. In particular, CIC protocols take forced checkpoint to prevent the creation of *useless* checkpoints, *i.e.* checkpoints that will never be part of a consistent global state

   [2]. CIC protocols do not need to send any special coordination messages like other protocols.

II. RELATED WORK

Arup Acharya and Badrinath, 1994 [3] presented a checkpointing protocol in which stable storage of MSS's is used by mobile hosts to handle the storage issue. In this approach each MH needs to take checkpoint in three cases *i.e.;* before moving to new cluster, before moving away from that cluster and during two phase rule. The two phase rule describes when a checkpoint should be taken. Therefore, this rule ensures that there is no dependency between two checkpoints.

Taesoon park and H.Y. Yeom, 2000 [4] proposed an algorithm in which message logging and dependency tracking is performed by MSS instead of MH to handle storage problem. There is no need of coordination amongst mobile hosts and there is no chance of failure. Moreover, the system can handle multiple and parallel failures.

Guohong Cao and mukesh Singhal, 2001 [5] introduced mutable checkpoints. To minimize the overheads incurred during coordinated checkpointing such as domino effect, a new scheme called *mutable checkpoints* has been introduced, which is neither tentative nor permanent and can be saved anytime and anywhere *i.e.,* local disk or MSS. Thus, mutable checkpoints are beneficial over uncoordinated checkpointing and coordinated checkpointing because of reduced storage overheads.

Tong- Tony –Chang, 2000, [6] presented an efficient recovery algorithm for cluster-based structure. Clusters are communicating with each other via cluster heads, which are the coordinator of all the nodes present in that cluster. Moreover the author has used the combination of checkpointing and rollback recovery. Each Processor maintains a log for saving its state and updates it from time to time. In case of any failure the process will start from its latest saved state..

Sapna E. George, Ing-Ray Chen, Ying Jin, 2006 [7] presented movement based checkpointing and logging for recovery in mobile computing system. In this approach, if a mobile host has changed its cluster a particular number of times called threshold then only checkpoint is taken where, threshold is function of log arrival rate, failure rate, mobility rate [13]. To calculate this value (threshold), a special model has been designed. Independent checkpointing and message logging is being combined in this protocol enabling asynchronous recovery of a node and also optimize recovery cost, recovery time and storage issues.

A. K .Singh-P. K. JAGGI, 2011 [8] presented a coordinated checkpointing scheme in which self stabilizing spanning tree are used to reduce the message overhead and also handle dynamic nature of MANETs. Staggered checkpointing approach was introduced to reduce resource contention. This protocol does not need FIFO channels and logs minimum number of messages .It supports concurrent checkpoint initiation and successfully handles the overlapping failures in mobile ad hoc networks [13].

Jaggi-Singh, 2011 [9] presented a protocol in which self stabilizing trees are used to take screenshot. As spanning tree finds shortest path between nodes, so all the cluster heads organize themselves in a spanning tree to reduce useless messages. This approach increased the number of cluster heads due to small size of clusters but also reduced number of messages to significantly low number. Moreover this scheme works efficiently in dynamic topology.

Tuli-kumar, 2011 [10] proposed a minimum process checkpointing scheme for clustering protocols. This algorithm fulfill the need of ad-hoc environment In this protocol whenever the cluster heads send routing and other collected information to the base station, it saves the information about the cluster heads in it. Here all the processes need not to take checkpoint. Whenever any base station is able to detect that a cluster head is failed, a new mobile host is being made cluster head. Therefore this approach reduces the energy consumption and recovery latency in case of cluster head failure.

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

Suparna Biswas et. al, 2012 [11] proposed a mobility based checkpointing and trust based rollback recovery for fault-tolerance in MANETs. A count variable is maintained to calculate number of clusters movements a mobile makes during one checkpoint interval. A threshold value is defined that defines the predefined value and is fixed as 3 and if that variable crosses that threshold value, the node takes checkpoint immediately. The proposed approach resulted in low recovery cost and high recovery probability of failed mobile hosts [13].
Suparna Biswas and Priyanka Dey, 2013 [12] proposed trusted node based secure checkpointing in MANETs. The author proposed a hybrid model in which encryption is being used for security. Results show that encryption is not efficient if checkpointing data is being forwarded through trusted nodes. Therefore non applicability of encryption reduces energy consumption of nodes and bandwidth consumption of links therefore increases applicability of this model in MANET environment with least resources.

III. PROPOSED METHODOLOGY

Trust Node Evaluation

Trust of a node is evaluated based on the trust level of the cluster in which the node is present on a particular instant of time and the cluster change count threshold value.
Trust value of each cluster is estimated on the basis of the number of trustworthy nodes present in the cluster.
Trust value of the cluster = [(∑ trust value of each node in the cluster)/ number of nodes in the cluster]
As, seen from the above formula, the trust value of the nodes in the cluster increases, the trust value of cluster also increases.
The increment in the value of the count (instead of simply incrementing the count by 1) when a node moves from one cluster to another is also dynamic and depends on the trust value of the cluster, i.e. if the node moves to a cluster having higher trust value, then the count value of the cluster is increased by a smaller value and vice-versa. So, cluster change count and trust value of the cluster are inversely proportional to each other.
Also, the cluster head selection is based on the trust value, energy of the node and number of times the node transmits the packets unsuccessfully (which should be minimum).

Check pointing

The value of the cluster change count threshold when a node moves from one cluster to another cluster is dynamic, means if the value of cluster change count of a node is greater than threshold the node is said to be prone to attack or unsafe to transfer secured information. At this time instant node which is attack prone can save its data to some trustworthy node of that cluster (either it is cluster head or some other node in the cluster) which is also termed as check-pointing node.

Recovery Mechanism

If a node is found to be malicious and required to be recovered then:

First the recovery node sends a signal to every cluster head to find the check-pointing node and cluster head further forwards the signal to all the nodes in the cluster.

The node containing the check-pointing data forwards the data to the recovery node needs to find the optimal route to transfer its data. The calculation of the optimal route is based on many factors like, the optimal route contains all the trusted nodes (cluster head or gateway node), consumes less energy to transfer the data.
The optimal route calculation is done with the help of some machine learning algorithm which takes these factors as its weight and iteratively calculates the optimal solution and dynamically changes its properties as per the requirement of the network.

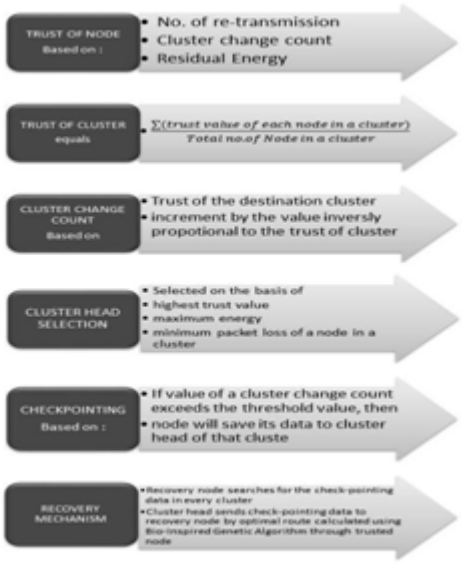

Figure 2. Methodology

IV. PROOF AND DEFINITION

Theorem: Check pointing data is recovered only through trusted nodes.

Explanation: Following two lemmas helps in proving the theorem

Lemma 1: Saving of Check pointing Data

The check pointing data is stored only in the cluster heads. The nodes which are selected as cluster heads are the most trusted nodes (having highest trust value) of the cluster along with the highest residual energy. Along with this, other criteria i.e CH nodes are assumed to be least mobile and placed at almost equal distance from every other node of the cluster. If the check pointing node may not be the CH before the recovery, still it has sufficient energy to store data for longer period of time.

Lemma 2: Check pointing Data Recovery

The recovery node must be either the CH of the cluster where a

978-93-85670-72-5 © 2016 (RTCSIT)
CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

node fails or the node with higher trust value. The path from the recovery node to the checkpointing node is only through trusted and energy efficient nodes which we obtained from the genetic algorithm.

Theorem: Trust of a node depends on its previous interactions with other nodes
Explanation: Following lemma helps in proving the theorem

Lemma 1: Opinion Dynamics
According to opinion Dynamics Algorithm the trust of a person depends on the opinion of its society and its previous interactions with other people. This algorithm can be applied to update the trust of a node.
Lemma 2: As the trust of a node depends on the previous interactions so a node is considered to be trustworthy if the number of retransmissions from that node is minimum and the trust also depends on the cluster in which the node is currently present which proves its social acceptance.

Theorem: Variable Cluster Change Count reduces the overhead from the CH

Explanation: The cluster change count is an important parameter for checkpointing. If it increases from a particular threshold, node needs to store its checkpointing data in the CH of the cluster in which it is currently present as the node is considered as prone to attack. If it increases with a fixed value then the node have to frequently store its data in the CH. By varying the count and reducing the increment factor, a node can cover more clusters without storing its checkpointing data thereby reducing the overhead from the CH. This increment factor depends on the cluster trust of the cluster in which the node is currently present. If the cluster trust is higher (or above threshold) the cluster change count increases with a lesser value and vice versa.

RESULTS AND DISCUSSIONS

1. Probability of Recovery: The probability of a node to be recovered is defined by probability of recovery. It depends on the trust value of a node and the cluster change count. If the cluster change count is high and the trust value is low, then the probability of recovery is high.

2. Residual Energy: Residual energy is the energy left at each node in the network after transmission and reception of packets by the nodes in the network. It is used to define the Network Lifetime of a node in the network. If the residual energy of a node in the network is less than the threshold, then the node is considered to be faulty or it is dead node.

3. Trust: Trust of a node is used to define the confidence on a node participating in the communication over the network. It measures the cluster change count which is the factor responsible for checkpointing of data and recovery.

Figure 3 and 4 shows the comparison graphs of the proposed methodology. In figure 3 residual energy is compared with respect to the simulation time and in figure 4 probability of recovery is compared with respect to the simulation time.

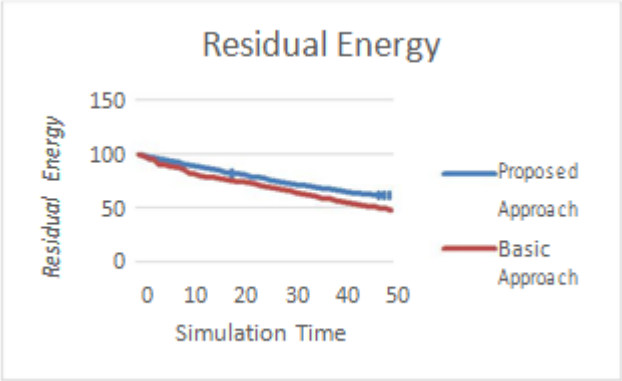

Figure 3. Residual Energy vs Simulation Time

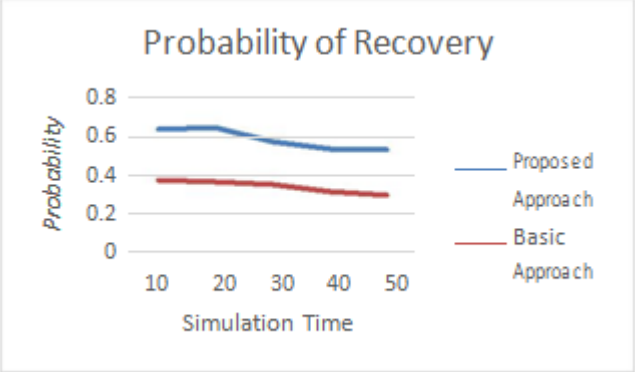

Figure 4. Probability of Recovery vs Simulation Time

CONCLUSION

In this paper we have reviewed some basic concepts of MANET and presented a new efficient movement based checkpointing technique. Different checkpointing approaches have been discussed. Clustering methods allow fast connection and also better routing and topology management of Mobile Ad-Hoc Networks. This paper 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. An example execution has been given to prove the static correctness of the protocol and graphical results has been shown.

ACKNOWLEDGMENT

I would like to take this opportunity to express my profound gratitude and deep regard to my supervisior Mr. Jasveer Singh for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

valuable suggestions were of immense help throughout my project work. Working under him was an extremely knowledgeable experience for me.
I would also like to give my sincere gratitude to my parents and friends for their valuable support and encouragement during this work, without which this research would be incomplete.

REFERENCES

[1] Abdul Shabbir, Anasuri Sunil Kumar (January 2012). "An Efficient Authentication Protocol for Security in MANETs" (PDF). *IJCCT* **3** (1): 71–74.

[2] Elnozahy, Elmootazbellah Nabil, et al. "A survey of rollback-recovery protocols in message-passing systems." *ACM Computing Surveys (CSUR)* 34.3 (2002): 375-408.

[3] Acharya and B.R. Badrinath, "Checkpointing Distributed Applications on Mobile Computers", *3rd Int'l Con. On Parallel and Distributed Information Systems, Oct. 1994, pp.* 73-80.

[4] Taesoon Park and Heon Y. Yeom , "An asynchronous recovery scheme based on optimistic message logging for mobile computing systems", 20th International Conference on Distributed Computing Systems, 2000, pp. 436-443.

[5] Guohong Cao and Mukesh Singhal, "Mutable Checkpoints: A New Checkpointing Approach for Mobile Computing Systems", ieee transactions on parallel and distributed systems, vol. 12, no. 2, february 2001.

[6] Tong-Ying Juang et al. , "An Efficient Asynchronous Recovery Algorithm in Wireless Mobile Ad hoc Networks" , International Conference on Communications in Computing CIC , June 25~28, 2001.

[7] Sapna E. George et al., "Movement-Based Checkpointing and Logging for Recovery in Mobile Computing Systems", InProc of MobiDE'06 , june 2006 , pp. 51-58.

[8] A. K .Singh and P. K. JAGGI "Staggered Checkpointing and Recovery in Cluster Based Mobile Ad Hoc Networks", International Conference on Parallel, Distributed Computing technologies and Applications (PDCTA-2011) Springer Proceedings, 2011.

[9] P.K. Jaggi and A. K. Singh , "Message efficient global snapshot recording using a self stabilizing spanning tree in a MANET", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 3, December 2011, pp. 247-255.

[10] R. Tuli and P. Kumar, "Minimum process coordinated Checkpointing scheme for ad hoc Networks", International Journal on AdHoc Networking Systems (IJANS) Vol. 1, No. 2, October 2011 ,pp. 51-63.

[11] Suparna Biswas et. al., "Mobility based checkpointing and trust based recovery in MANET", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 4, August 2012.

[12] Suparna Biswas and Priyanka Dey, "Secure Checkpointing-Recovery Using Trusted Nodes Nn MANETs", 4th International Conference on Computer and Communication Technology (ICCCT), 2013.

[13] Shefali Aggarwal and Dr. Poonam Saini, " Checkpointing in mobile ad hoc networks (MANETs)- A survey" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India