International Journal of Computer Networks and Applications (IJCNA)
Volume 2, Issue 4, July – August (2015)

RESEARCH ARTICLE

Dynamic Node Recovery in MANET for High Recovery Probability

Ravneet Kaur
Research Scholar, CEC Landran, Mohali, Punjab, India.
brarravneetkaur@yahoo.in

Dr. Neeraj Sharma
Head of Department (CSE), CEC Landran, Mohali, Punjab, India.
csem.csehod@gmail.com

Abstract – One of the key design issues in ad hoc networks is the development of rollback recovery model for providing fault-tolerance in MANET. Because the potential problem of MANET is limited energy, probability of fault occurrences is more. Hence, checkpointing is done at trusted nodes when faults are encountered, for successful rollback to the last saved state. This makes trust a vital factor to be determined. The proposed algorithm aims to reduce the rollback recovery time by retrieving the checkpoint data through trusted nodes. Dynamic node recovery technique unfolds the impact of cluster trust on the count variable maintained by each node. This variable is so maintained, to do the checkpointing process when a definite threshold is reached. Such an attack prone node saves its data at the nearest trusted cluster head. Again, based on opinion dynamics, trust of the host cluster markedly influences the trust of the visitor node. Moreover, genetic algorithms are employed to search best optimal recovery path. Performance analysis depicts remarkable results produced by the proposed algorithm.

Index Terms – MANET, count, checkpoint, trust, GA, recovery.

1. INTRODUCTION

MANET is a wireless collection of mobile nodes with a dynamic topology thereby rapidly changing the structural space of nodes. It does not rely upon any fixed infrastructure or underlying network. Each node in an ad hoc network can behave as a host as well as a router. Although such nodes are confined to short range and limited energy levels, but MANET is a very flexible structure with its suitable applications in networks requiring temporary and instant connection. MANETs are usually deployed in harsh and severe uncontrolled environments, thereby increasing the probability of compromises and malfunctioning as there is no centralized control to monitor the node operations [9]. A mobile node has a certain transmission range confined to a circular space around itself. The radius of this range depends upon the intensity of its power, receiver sensitivity and propagation loss. When the source has to transmit data to the destination node that is not within its transmission range, then it uses the intermediate nodes to reach the destination. This way MANET behaves like a multi-hop network. Data travels through multiple hops in order to offer network connectivity in such scenarios. The nodes in MANET congregate to form up a cluster, such that the all the individual clusters can be together viewed as a single large system. Clustering is highly favorable in large and high mobile networks where scalability is of great significance. Every cluster has a nominated Cluster Head (CH) and a gateway node. All other nodes in the cluster except these two are called as ordinary nodes. Gateway node is responsible for inter-cluster communication i.e., forwards the data packets between two clusters. CH is the local coordinator of its cluster such that it is responsible for all the communications within that cluster and with other clusters as well. One CH is chosen per cluster. Various schemes have been proposed that considers one or more among several factors like location of node, trust, energy, failure rate, availability, mobility, etc. as the principles of election. But most probably, trust value of a node and its position within the cluster are given priority. Trust can be defined as a belief in a node that it is reliable and is available in the network for a longer time period. It is defined as the subjective evaluation by similar nodes whether the node is able to transmit data or not. Literature works contributed plenty of definitions of trust but none of these provide satisfactory statement to it. It is referred to as an element of availability, reliability, energy and several other trivial aspects, but none of these describe trust well because trust is an abstract concept [16] which is a blend of many complex factors. In a cluster, a trusted node is able to exist in the network for a longer time period because it has sufficient battery power to persist. Also, such a node is failure free. Quantifying trust on trust scale, trust ranges from 0 to 1. 0 exhibits a distrusted node and 1, a trusted node [20]. Computation of trust value is a difficult challenge to be faced because of diverse distinctive features influencing it. Thus, trust is a vital property to be determined for a node.

Fault-tolerance in MANET is an important design issue. Faults like node failures, network failures, misbehaving nodes, power reduction, etc. often occur in such networks. A fault-tolerant system is able to withstand in event of such failures. This property ensures that the malfunctioning node does not affect the whole system. It is the ability to handle unpredicted software and hardware failures. Once the failure occurs, appropriate measures are taken to resist any unwanted

RESEARCH ARTICLE

changes. In order to make a system fault-tolerant, checkpointing based rollback recovery is done. Checkpointing process ensures a fault-tolerant system by saving data and current process state of the failed node at some secure sphere. When the failed node recovers, it may resume its computation by rolling back to the last saved checkpoint. This saves time to go up again to the initial execution point of the process. Several limitations such as restricted energy level, storage space and bandwidth makes the checkpointing process difficult to employ in real environment. Usually, checkpointing is done on some trusted node i.e., a trustworthy node within a cluster acts as the recovery or backup node for the failed node and as already discussed above, CH is the one that is most trusted. So, an attack prone node locates all of its data on the current CH. The checkpointing data is carried from the recovery node to the failed node through the intermediate nodes. Again, these nodes should also be trusted so as to successfully conclude the recovery process.

In the proposed research work, we have addressed the major problem of node failures encountered in ad hoc networks and proffered a precise and efficient approach to deal with it. We present a dynamic data recovery technique to build a fault-tolerant network in MANET. Such a fault-tolerant network persists into a consistent state of nodes. Proposed algorithm constructs a reliable system against anticipated node failures. The manuscript sections are organized as: Section 2 discusses the major relevant literature findings. Section 3 is the detailed presentation of the proposed research. Implementation results of the above research are analyzed in section 4. Next segment features brief conclusion followed by references, bringing the paper to its extremity.

2. RELATED WORK

Presented below are some of the literature works that employed respective checkpointing and recovery procedures in case of node failures in MANET.

Mobility based fault-tolerance technique has been proposed by S. Biswas et al. [10]. It makes certain that only trusted nodes constitute the recovery path so as to ensure successful retrieval of checkpoints. Similarly, only a trusted node is chosen as a CH. Each node in the network maintains a count variable which is incremented by a certain value every time a node visits a new cluster. The incremental factor in the proposed algorithm is 1. Checkpoints are taken at the current CH when this count value becomes greater than a pre-defined threshold value. Trust value of a node is computed based upon 4 influential factors namely, failure rate, energy, availability within a network and recommendations from the neighboring nodes. The proposed algorithm overcame various existing limitations however, several other important aspects like security of checkpoints are being ignored. Another research work proposed by S. Biswas et al. [11] emphasizes the importance of trust and belittle the significance of encryption technique required for checkpoint recovery. It ensures that if only the trusted nodes make up a recovery path then encryption of checkpoints is inessential because a trusted node will not result into failure. In the worst scenario, if a node finds next node in the path to be distrusted then it encrypts the checkpoint and sends it along the remaining recovery path. Once encryption is done, the remaining path nodes need not perform any further verification of next node in the path with respect to its trust level. In such instances, the most inconvenient job is to maintain the cryptographic keys. The above research team further proposed an ant colony optimization technique for checkpoint recovery [7]. Aforementioned technique is similar to the ant's food fetching technique. For hunting an optimal food path, ants use pheromone to provide information regarding its intensity along a path. Higher the pheromone intensity more is the likelihood of the path to be selected. Likewise, in MANET, a dummy packet is first sent along some path. If it is successfully received at the destination along that path, then its pheromone amount is increased. So, a path with high density of pheromone amount is the most favorable path for recovery. No encryption overheads are incorporated in the proposed work, although use of dummy packet requires extra energy. Apart from this, pheromone list must be periodically updated.

A. K. Singh and P.K. Jaggi [3] proposed an asynchronous recovery technique in which checkpoints are taken on the current CH based upon virtual region. The current CH and its immediate neighboring clusters build up a virtual space. When MH leaves virtual region then only checkpointing is done at the new CH. P. Gera et al. [4] considered security of checkpoints as the prime factor wherein safe connection is provided along transmission and routing phase. Along the transmission phase, component parts of data are fragmented, self-encrypted and are sent along different paths. Self-encryption prevents the maintenance of keys information, thereby, minifying the computational process. Along routing phase, sensitive information about the fragmented parts is sent along a path consisting of trusted nodes only. The proposed algorithm sets up much secure routing path but is unhandy to realize in practical. X. Li et al. [1] proposed checkpointing scheme based on a single key factor, sojourn time. Sojourn time is the transitory stay time for which a MH stays at a Mobile Support Station (MSS). Research team considered it as the only factor based upon which checkpointing should be done. Thus, the probability of checkpointing increases if MH stays at MSS for a longer duration. Even though much superior outcomes were incorporated but more checkpointing data is accumulated this way which may lead to unwanted failures. An existing TARF concept (Trust Aware Routing Framework) is congregated with the BLME technique (Backup Link Mutual Exclusion) by P.P. Rewagad et al. [17] for node recovery. TARF approach is responsible for the

RESEARCH ARTICLE

detection of identity frauds and prevents them. It chooses recovery path of trusted nodes only. In case of dual-link failures, BLME generates two mutual exclusive backup paths for recovery. R. Tuli et al. [5] presented an asynchronous checkpointing and optimistic message logging scheme. In order to overcome low storage capacity of a mobile host (MH), memory region of CH is utilized as stable storage of data by a MH. MH is then concerned with minimum information only, effectively utilizing its short storage. CH keeps a track record of messages for every node within its cluster. MH can voluntarily leave a cluster in order to conserve energy. This is termed as 'disconnection'. The above approach is optimistic such that the MH does not wait for a process to be complete before sending the next message and assume an absolute logging process. The proposed scheme delivers better performance but at times, may create orphan messages. In the proposed OTMF (Objective Trust Management Framework), trustworthiness metric is a composite value of trust as well as confidence value of a node [24]. It is an objective computation, where confidence value refers to the accuracy of trust value. Comparison with the existing reputation-based framework has been made depicting the necessity to include confidence value in the computation of trustworthiness because its presence and absence changes the trust value invariably. Although both the approaches provide admirable impartial conduct of node towards its neighbors, but more rational framework can be built using the proposed model.

3. PORPOSED MODELLING

In the proposed research work, we analyzed the influence of trust in a clustered network and an appreciable amount of affect has been produced as a result. Additionally, we employed genetic algorithms for finding the best recovery path consisting of trusted nodes only.

Each mobile node is in charge of a count variable whose numeral value when becomes greater than a presumed default value, and then checkpoint data of that node is saved at some trustworthy node. The count variable updates according to the trust value of the host cluster which it joins during mobility. Unlike existing approaches, the change observed is dynamic i.e., count always increments by a variable value. This variation in value depends upon the trust level of a cluster such that for higher cluster trust, the increment is lower and for lower cluster trust level, the increment observed is higher. Thus, both being inversely proportional to each other bring about a dynamic change in the count variable. Cluster change count value is noteworthy because it discerns the failure rate of a node. Again, cluster trust also influences the trust value of the visitor node. A node entering into a cluster with high trust has positive impact on its trust value. On the other hand, lower cluster trust level has negative effect. This impact is realized by altering the trust of the visitor node by a marginal value.

Apart from this, genetic algorithmic approach is utilized to find an optimal path between the recovery node and the checkpointing node for successful transmission of checkpoint data between the two. An ideal path with trustworthy nodes and high residual energy is chosen from a number of feasible paths. Fitness function determines the reliability of the path. Higher fitness recovery path is chosen.

The proposed research work progresses through following phases:

3.1. Evaluation of trust for a node

Each node in a cluster is assigned some initial trust value. These trust values of individual components of a cluster constitute cluster trust. It is calculated by dividing the summation of trust of all the cluster nodes with the total number of nodes within that cluster. So, nodes with higher trust value within a cluster are an evidence of higher cluster trust. Now, a node with higher trust level is nominated as CH. The other two concerned factors related to election of CH are energy and packet loss. Thus, a node which has higher trust value, maximum energy and minimum packet loss with respect to other nodes in the cluster is elected as CH.

When a mobile node visits a host cluster, two factors are liable to change. One is the change in its trust value and the other is the change in its count variable.

Trust of visitor node is revised to a new value upon entrance in new cluster. This is done based upon opinion dynamics. If the trust of the host cluster is a greater than the trust of the visitor node then the trust of the visitor node increases by a minimal value of 0.002. This is an edge provided to such a node for entering a trustworthy cluster. Conversely, decrement of corresponding measure is observed.

The change in count variable is dynamic and depends upon the trust level of the cluster. The cluster change count is inversely proportional to the cluster trust i.e., when a node enters into a cluster with higher trust, then the count decreases by a value inversely proportional to cluster trust value. So, higher the trust, smaller is the change observed. This concept is a variant of existing algorithm [10] where the increment is made by a constant value i.e., 1, every time a node visits the host cluster. The former proposals by research scholars considered an increment of 1. However, we consider that cluster trust is a major influential factor that affects trust of a node present in that cluster at a particular time instant.

3.2. Checkpointing

As discussed above, the change in the count variable is dynamic. When the count variable value approaches towards a pre-defined count threshold, probability of the node to be attack prone becomes greater. When the increasing count number exceeds the threshold value, checkpointing is done at some trustworthy node. Usually, current CH is elected as the checkpointing node which preserves the process' information of the failed node.

RESEARCH ARTICLE

3.3. Recovery

An attack prone node can fail at any time. Failure of a node may partition the network into discrete structures and can affect the whole communication. So, quick retrieval of checkpoint data should be done upon failure so as to avoid an abrupt disconnection of the mobile node with the remaining links.

The recovery node sends request to each CH in the network, asking for the checkpoint data saved by it earlier at the current CH at that very point of instant. The checkpointing CH that held the checkpoint data responds with an acknowledgement of possession. Then an optimal route between the checkpointing node and recovery node is found so as to transfer the vital checkpoint information. Only trusted nodes are chosen for this purpose. We have employed genetic algorithm to find the best path between the two ends.

Genetic algorithm (GA) is a search heuristic approach that generates best optimal solution to the search problems from a set of possible solutions by imitating the natural evolution processes. Genetic operators like crossover and mutation are applied to produce next new generation. Fitness function is an objective function that assesses the quality of a potential solution with respect to other candidate solutions. Each individual is assigned a fitness value that depicts its ability to compete. Based on the fitness value, new breed of solutions is created. One with higher fitness breeds through to the next generation. The fitness definition varies from problem to problem. Fitness function used in the proposed work is

Fitness function (f) = $T * w_1 + E * w_2 + (1- R_{t)} * w_3$

Where T is trust of a node,

E is residual energy of a node,

R_t is packet retransmission rate,

w_1, w_2, w_3 are the respective weights depicting the influence of corresponding factor.

Thus, fitness function is directly proportional to trust and energy of the nodes and inverse to the packet loss rate.
A genetic process proceeds through following stages:

- Initialization: First, random initial population is generated. This population can vary from hundreds to thousands of feasible solutions. All the random initials constitute a search space.
- Selection: Each individual solution is provided with a fitness score. From the existing set of solutions, ones with better fitness breed into new generation. So, certain proportion with better fit solutions makes up new offspring.
- Crossover: Individuals selected in the above stage operate under the crossover process. A random crossover point is chosen from the string of bits. The string values up to this point are swapped and the resulting string is the new offspring. In the proposed work, half of the selected individuals are executed under crossover process.
- Mutation: Mutation process is put into effect after crossover is performed. Certain bits are randomly flipped for obtaining a global optimum, thereby maintaining genetic diversity among generations. Bit values are switched between 0 and 1.

The above steps are repeated until a best solution is obtained.

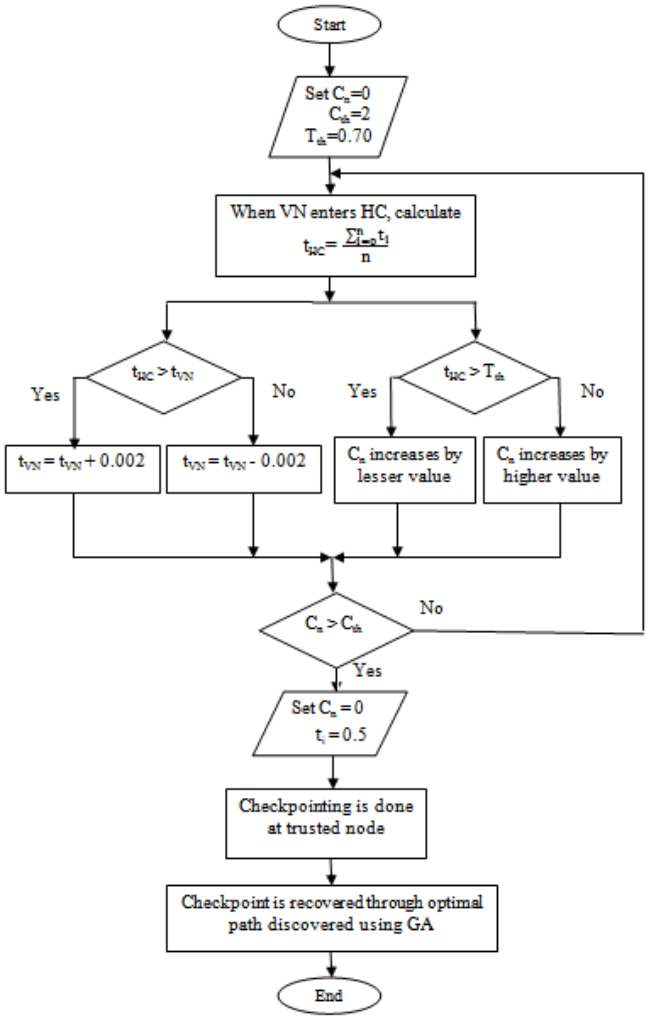

Figure 1 Proposed Research Modelling Diagram

Algorithm for proposed research work:-

1) Start

2) Set initial count variable of each mobile node to zero i.e., $C_n = 0$
Where n=1, 2…50

3) Set $C_{th} = 2$

RESEARCH ARTICLE

4) Set $T_{th} = 0.70$

5) Assign initial trust t_i to all nodes, where t_i is the trust of i_{th} node

6) For each cluster calculate trust of host cluster, t_{HC}

$$\text{cluster trust} = \frac{\sum_{i=0}^{n} t_i}{n}$$

Where n is the number of nodes in the cluster

End for each

7) When visitor node (VN) enters new host cluster (HC), update its trust based on opinion dynamics

if ($t_{HC} > t_{VN}$)

t_{VN} increases by 0.002

else

t_{VN} decreases by 0.002

end if

where t_{HC} is trust of HC

t_{VN} is trust of VN

8) For each node n

if ($t_{HC} > T_{th}$)

C_n increases by a lesser value (i.e., trust of host cluster)

else

C_n increases by a higher value (i.e., trust of host cluster)

end if

end for each

9) if ($C_n > C_{th}$)

Node n saves its checkpoint data at the current CH

Set $C_n = 0$

Set $t_i = 0.5$

end if

10) After failure, in order to recover the checkpointing data, recovery node sends request to each CH for the checkpoint.

11) Corresponding CH_{chk} sends CH_{ack} to the N_{rec} where N_{rec} is the node to be recovered (recovery node)

CH_{chk} is the checkpointing node at which N_{rec} preserved its checkpoint before failure

CH_{ack} is the acknowledgement sent by the CH_{chk} to the N_{rec} regarding maintenance of checkpoint held by it.

12) Apply GA

-Initialize random population of candidate solutions, t

-Evaluate fitness function f

For each trusted route possible between CH_{chk} and N_{rec}

Assign binary value to each node

Based on f, select two candidate solutions from t

Perform crossover to produce new offspring population (t+1) at crossover rate of 0.5

Perform mutation on new offspring (t+1) at muattion rate of 1.0

Evaluate fitness of new population

Create new population of new offspring (t+1)

-Repeat above steps untill best value path is obtained.

end for each

13) Checkpoint is recovered through the optimal path discovered

14) End

4. RESULTS AND DISCUSSIONS

Efficiency of the proposed research work has been evaluated using NS2 simulator. 50 nodes, assembled together into 5 clusters, operate within a topology grid of 800*800. Random way point model is used as the mobility model and DSR (Dynamic Source Routing) is the routing protocol used. Unlike the existing approaches, we consider the count change as dynamic. Initial set value of cluster change count variable for each node is 0. This count is incremented by a dynamic value every time it visits a new cluster. This change is inversely proportional to the trust value of the new cluster in which it enters such that if the trust value of new cluster is a high value, count variable changes by a low value and vice-versa. Another change observed is in the trust value of the visitor mobile node. If the visitor node enters into a cluster with cluster trust value greater than 0.7, then the trust of the visitor node increases by a modest value of 0.002. Contrary, if the trust value is below the threshold of 0.7, then the trust of the visitor node decreases by the same measure.

Moreover, the presumed threshold of the count variable is taken as 2. In other words, when the count value of a node becomes more than 2, then checkpointing process is carried out by that node. The count value of such attack prone node is again set to zero value after the checkpointing is done. Its trust is also lowered down to a negligible value of 0.5. With respect to genetic algorithm, 0.5 and 0.1 are the respective crossover and mutation rates.

To be precise, following is the parameter set that outline the conditions of operation in the simulation environment.

RESEARCH ARTICLE

Parameters	Values
Routing protocol	DSR
Mobility model	Random Way Point Model
Total number of nodes	50
Topology grid size	800*800
Initial energy of a node	100
Count threshold	2
Count increment of visitor node	Inversely proportional to trust of the host cluster
Increment/decrement in trust value of the visitor node	0.002
Crossover rate	0.5
Mutation rate	1.0

Table 1 Simulation Parameters and their Corresponding Values

4.1. Performance Metrics

Recovery probability and Residual energy of a node are the two performance evaluation metrics used to assess the effectiveness of the proposed research work.

(i) Residual Energy

Residual energy is the leftover energy of a node while progressing through a network. Each node has some initial energy which depletes as the mobile node travels from one place to other. Abstraction of consumed energy from the initial energy forms up residual energy. So, lesser the consumption, higher is the residual energy, more is the lifetime of network.

(ii) Failure Recovery Probability

Failure recovery probability of the failed node is the probability of regaining the last saved state of its processes. This is done so as to resume the processes and reduce the computational time when node failure occurs which would otherwise require all the processes to be executed from beginning. Higher probability of recovery results into high throughput of the system.

4.1.1 Residual Energy

In the proposed algorithm, the residual energy of a node goes to a minimum of 62 and the slope first goes down at a sharp angle but after a certain time period it becomes constant. This improves the network lifetime of the nodes as the residual energy in the proposed algorithm lasts for a long time.

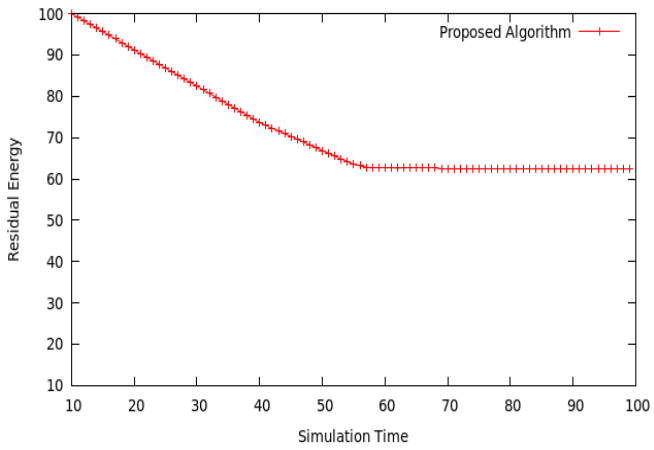

Figure 2 Residual Energy v/s Simulation Time

4.1.2 Failure Recovery Probability

Probability of Recovery in the proposed algorithm forms a stable curve where it goes down to a minimum low value of 0.5. The probability again improves after this drop. Thus, this depicts the efficiency of the proposed algorithm as it maintains an exceptionally fine recovery level.

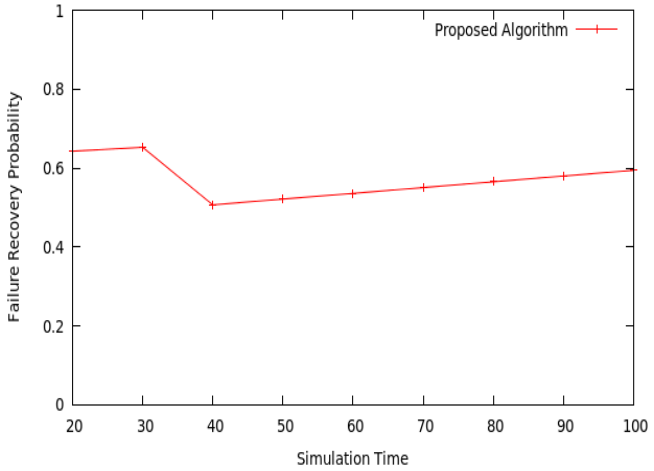

Figure 3 Failure Recovery Probability v/s Simulation Time

Above presented evaluation of simulation results clearly depicts how the proposed work outperforms several existing algorithms. The desirable improvements in the existing approaches have been made building up a much effective fault-tolerant model. Relatively, much low recovery time is consumed by the proposed algorithm for recovery of checkpoints.

5. CONCLUSION

A dynamic node recovery technique has been proposed in this paper that ensures quick retrieval of checkpoint data to build fault-tolerant network in MANET. The proposed algorithm

RESEARCH ARTICLE

effectively employs genetic operators to find the best optimal path for recovery. This path comprises of trustworthy nodes only. Thus, trust element of a node is a salient feature that considerably contributes towards construction of a durable network. In the proposed work, trust of a cluster has notable effect upon trust of the visitor node and its count variable such that the reflected change in count is dynamic. This approach significantly improves lifespan of network as the residual energy of nodes fall down gradually. Moreover, low recovery time enhances throughput of the system. Certain other prominent propositions of recovery can be further explored in the near time.

REFERENCES

[1] X. Li, M. Yang, C. Men, Y. Jiang, and K. Udagepola, "Access-Pattern Aware Checkpointing data storage scheme for mobile computing environment," Procedia Computer Science, 34 (2014) 330 – 337, Elsevier, 2014.

[2] D. Gavalas, G. Pantziou, C. Konstantopoulos, and B. Mamalis, "Clustering of Mobile Ad Hoc Networks: An Adaptive Broadcast Period Approach," unpublished.

[3] A.K. Singh, and P.K. Jaggi, "Asynchronous Rollback Recovery in cluster based Multi Hop Mobile Ad Hoc Networks," International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471, vol. 2 issue 6, June-2013.

[4] P. Gera, K. Garg, and M. Misra, "Trust-based Multi-Path Routing for Enhancing Data Security in MANETs," International Journal of Network Security, vol.16, no.2, pp. 102-111, March 2014.

[5] R. Tuli, and P. Kumar, "Asynchronous Checkpointing and Optimistic Message Logging for Mobile Ad Hoc Networks," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 2, no. 10, 2011.

[6] C.M. Jadhav, A.R. Shegadar, and S. Shabade, "Dual-Link Failure Resiliency through Backup Link Mutual Exclusion," International Journal Of Engineering And Computer Science, ISSN:2319-7242, volume 3 issue, December 2014.

[7] S. Biswas, P. Dey, and S. Neogy, "Trusted checkpointing based on Ant Colony Optimization in MANET," Third International Conference on Emerging Applications of Information Technology (EAIT), 2012.

[8] P. Sharma and N. Khurana, "Study of Optimal Path Finding Techniques," International Journal of Advancements in Technology, vol. 4 no. 2, July 2013.

[9] K. Govindan, and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey,", IEEE.

[10] S. Biswas, S. Neogy, and P. Dey, "Mobility based checkpointing and trust based recovery in MANET," International Journal of Wireless & Mobile Networks (IJWMN), vol. 4, no. 4, August 2012.

[11] S. Biswas, P. Dey, and S. Neogy, "Secure Checkpointing-Recovery using Trusted Nodes in MANET," 4th International Conference on Computer and Communication Technology (ICCCT), 2013.

[12] 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.

[13] P. Sharma, and A. Khunteta, "A Survey of Checkpointing Algorithms in Mobile Ad HocNetwork," Global Journal of Computer Science and Technology Network, Web & Security, (USA), volume 12 issue 12, version 1.0, 2012.

[14] S. Behzadi and A.A. Alesheikh, "A Pseudo Genetic Algorithm for solving best path problem," The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, vol. 3,. part B2, 2008.

[15] Z. Ishrat and K.B. Ali, "Optimization of Route in a Network using Genetic Algorithm," International Journal of Computer Applications (IJCA), ISSN: 0975–8887, 2013

[16] R. Kaur and Dr. N. Sharma, "Checkpointing and Trust based Recovery in MANET: A Survey," Advances in Computer Science and Information Technology (ACSIT), ISSN: 2393-9907, May 2015.

[17] P.P. Rewagad, and S.R. Suryawanshi, "Implementation of Trust Aware Routing Framework with Link Failure Consideration and Recovery," International Journal of Research in Computer and Communication Technology, vol 3, issue 9, September 2014.

[18] A. Patnaik, L.K. Awasthi, and K. Dutta, "Analysis on Checkpointing Scheme Paradigms for Mobile Ad-hoc Network: A Review," IJCSC, vol. 3, no.2, January-June 2012.

[19] D. Maheshwari, and A.Dhanalakshmi, "Fault Tolerance in Mobile ad hoc Network: A Survey," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, issue 3, March 2013.

[20] R. Dalal, M. Khari, and Y. Singh, "Different ways to achieve Trust in MANET," International Journal on AdHoc Networking Systems (IJANS), vol. 2, no. 2, April 2012.

[21] B. J. Oommen, and L. Rueda, "Fault-Tolerant Routing in Mobile Ad Hoc Networks," www.intechopen.com.

[22] P. Aggarwal, "A Study on achieving Fault Tolerance in Mobile Ad-Hoc Networks (MANETs)," Journal of Global Research in Computer Science, ISSN: 2229-371X, vol. 4, no. 12, December 2013.

[23] J.W. Huang, I. Woungang, H.C. Chao, M.S. Obaidat, T.Y. Chi, and S.K. Dhurandher, "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks," IEEE Globecom, 2011.

[24] R. Li, J. Li, P. Liu, and H.H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," IEEE Vehicular Technology Conference, ISSN: 1550-2252, April, 2007.