International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 79-101
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

A Fault Tolerant based Efficient Power Route Discovery Approach for MANET

[1]A.K. Ashfauk Ahamed, [2]M. Anand Kumar and [3]B.L. Shivakumar

[1]Department of Computer Applications,

Kongunadu Arts and Science College,

Coimbatore, India.

[2]Department of Information Technology,

Karpagam University,

Coimbatore, India.

[3]Sri Ramakrishna Polytechnic College,

Coimbatore, India.

Abstract

In MANET, nodes are mobile which are connected without any centralized infrastructure. Because of the portability of mobilehubs, arrange segment happens. Moreover, network failures and link failures are occurred to degrade the performance of the networks. Hence, there is need for effective fault tolerant based routing. From the previous analysis, cluster based routing is deployed but not able to tackle faults namely node failures, link breakage and malicious activities. It will lead to more power consumption. To conquer this issues, we suggest to develop Cluster based Multipath Fault Tolerant Routing Scheme (CMFTRS) for determining power route among the network. This scheme consists of three phases namely multipath routing establishment, cluster head selection and fault tolerant routing. In our proposed plot, multipath routing is built up to make strides fault tolerance and system lifetime. In cluster head selection phase, the cluster members chose their cluster head based on their aggregate weight. Each cluster head maintain their neighbor table and fault tolerant table to obtain status of packets dropped, packets duplicated and packets received. In fault tolerant routing, link failures and network failures are isolated and packets are effective forwarded to the destination node. By utilizing system test system, the proposed conspire accomplishes better than our previous works namely EFDCB and FDCB.

Key Words: Cluster head selection, multipath routing, fault tolerant routing, aggregation weight, link failures, node failures, packet delivery ratio, network reuse ratio and overhead.

1. Introduction

Because of the nearness of mobility in MANET, hubs are randomly moving inside the region. This will lead to failures of path, link and misbehaving nodes are getting increases. To overcome this, several approaches [1-4] introduced fault tolerant routing that focus on single secure path, replication routing etc. But, communication overhead in theses papers are increased unlimitedly. In paper [5-7], authors focused on QoS based multipath routing, cluster routing, back off delay time to reduce the effect of path failures. In our paper, cluster routing is established initially, after that cluster head is chosen based on aggregate weight. While initialling these weights, high recommended cluster members can be chosen as a cluster head. In papers [8-11], fault tolerant routing, fault tolerant service discovery protocol, learning automata and proactive fault tolerant routing are proposed to secure the paths. But there is no mathematical analysis for the selection of optimized paths is given. In papers [13,14], distributed blame lenient directing and Cluster based blame lenient routing are proposed. But these papers are not focused on network connectivity and blame lenient routing. In our suggested cluster based multipath blame lenient routing, we have focused how to discover and maintain the multipath routing to achieve high network lifetime.

In cluster head selection method, we introduced the concept of aggregation weight to avoid the disqualified cluster members. In blame lenient routing, we introduced route selection and route evaluation methods. In these methods, the probability of delivery of packet rate is successfully estimated and selection of successful routes is identified. But in previous work, either cluster routing or blame lenient routing is considered. But in our article, the reason for combining these two papers is to avoid unnecessary overhead occurrence, path broken and malicious activity arises. The following issues arise from the malicious activities:

- **Broadcast errors**: The transmitted packets is getting corrupted and thus received in error because of the lack of quality of the remote medium and the capriciousness of nature.
- **Mobile Hub disappointments:** Due to various sorts of perilous conditions in the earth, hubs may come up short whenever. It might likewise drop out of the system either deliberately or when their vitality supply is exhausted.
- **Path disappointments:** Node disappointments and in addition changing natural conditions may bring about ways between hubs to break.
- **Ruptures of path**: Due to high dynamic topology rate, network and path failures occur rapidly. Packets are sent through stale courses may either in the long run be dropped or be deferred relying on the system transport convention.

- **Congested nodes:** Certain nodes may become congested due to the topology of the network and the nature of the routing protocol. This will lead to either larger delays or packet loss.

The commitment of this paper is as per the following:

- Multipath routing is proposed to improve fault tolerance and network lifetime.
- Packet delivery rate and selection of best route are determined in fault tolerant routing.
- Route discovery and route maintenance process are derived for proposed multipath routing.
- Route evaluation and Route selection are determined in fault tolerant routing.
- Packets are effectively forwarded in the presence of link and path failures.
- Aggregation weight to each cluster member in cluster is calculated.
- Network failures namely node failure, link breakages and malicious activities can be handled using proposed fault tolerant model.
- Cluster head is selected based on aggregate weight.
- Efficient Power Limitation Route is established based on fault tolerant condition.
- Each cluster head maintain their neighbor table and fault tolerant table to obtain status of packets dropped, packets duplicated and packets received.
- Various Qos parameters have been taken for simulation analysis which shows the better performance of proposed scheme.

The paper is sorted out as takes after. The Section 1 portrays presentation about MANET, review of network prone attacks and contribution of research work. Segment 2 manages the past work which is identified with fault tolerant and multipath routing. Segment 3 is given for the execution of proposed scheme. Segment 4 portrays the execution investigation and the last segment closes the work.

2. Related Work

In this paper [1], Adaptive Fault Tolerant Replication Routing (AFTR) convention was proposed to expand the estimation of bundle conveyance rate. The point of this convention is to perform single reaction metric investigation of AFTR utilizing three execution measurements to be specific throughput, Packet conveyance proportion and directing overhead under five noticeable elements like system size, transmission rate, portability speed, stop time and ideal number of duplicates utilizing factual approach named Taguchi's approach. Here they have not considered more QoS parameters to assess the execution of their proposed convention.

In [2], the activity be re-steered along a sub-path was recommended that bypasses a fragment of the essential path which contains the fizzled connection or hub. In addition, the recognizable proof of the fragments is not settled from the earlier but rather it is resolved in light of accessibility of interchange paths, and QoS limitations. This plan guarantees that if availability between a given match of hubs is sufficiently rich then for any essential path one can simply discover interchange paths in order to address the issue of connection or hub disappointment.

This adaptability in distinguishing the fragments can likewise be utilized to guarantee that the postponement in changing movement over to a substitute path, and the subsequent parcel misfortune, are limited. The principle absence of this approach, not considered multipath steering to spare the system lifetime. The issue of secure and blame tolerant correspondence was tended to [3] within the sight of intruders over a multi-bounce remote system with every now and again evolving topology. So as to adapt to discretionary vindictive disturbance of information transmissions, it was proposed the secure message transmission (SMT) convention and its option, the secure single-path (SSP) convention. SSP is the capacity to work exclusively in a conclusion to-end way and without prohibitive suppositions on the system trust and security affiliations. This convention exploits topological and transmission redundancies and uses input, traded just between the two imparting end-hubs. Here, creator is not considered on solid directing with bunch based approach. Additionally, the correspondence overhead of this convention increments boundlessly.

In [4], another metric for identifying the nature of fellowships was figured precisely. From this metric, every hub characterizes its kinship group as the arrangement of hubs having dear fellowship with itself either straightforwardly or in a roundabout way. In this work, Friendship Based Routing was presented in which transiently separated fellowships are utilized to settle on the sending choices of messages. For this reason, they have characterized new metric measuring distinctive parts of kinship practices and it was recorded in the historical backdrop of their experiences with different hubs. In addition, both immediate and aberrant fellowship was considered. It was likewise separated fellowships as indicated by time of day and proposes to utilize distinctive companionship groups in various eras. The issue here is, not concentrating on dependable neigh or or kinship hubs to forward the bundle. In [5],a disseminated blame tolerant directing convention was produced for QoS bolster in portable impromptu systems, which mitigates interruption time under system disappointments.

It was shown that the customary technique for rerouting QoS activity from the source given a connection disappointment yields genuine negative QoS disturbance outcomes. A productive neighborhood blame tolerant calculation can altogether alleviate the time required to re-build up an association. The reconnection time was lessened which goes for diminishing QoS activity. The

disadvantage of this paper is, the creator not concentrated on numerical investigation.

In [6], a change over group based directing was made with an aid of virtual node layer also, refreshing Ad hoc On Demand Distance Vector convention with virtual node layer. Here, it was implemented a cross layer based whereby the system layer will section or choose the bundle sending rate in light of evaluated data transfer capacity, data gave by Medium Access Control layer. Moreover, mainly it was dealt with upgrading AODV directing convention utilizing virtual nodes.

The main drawback is, the proposed scheme is only evaluated with AODV not other routing protocols. To combat against faults like network failure, link failure, It was designed that the SBAR protocol [7] based on space back-off defer time, including Expanding Ring Search system. It was likewise planned that versatile back-off postpone time equation. In the course answer strategy and the information transmission, self-determination calculation will be applied to improve a new forward method based back-off forwarding, in which the slot delay time will be applied, and it will be taken into account more factors affecting the performance of SBAR in computing the delay time. Here, the authors have not considered on balancing back-off delay time and packet delivery rate. In [8], the Fault Tolerant Routing Protocol (FRMR) was compared to build ways utilizing the vitality level in the hub. With the assistance of flooding the demand again through from the past hub, the bundles will be retransmitted. Regardless of the possibility that the way chose is by most limited way, it sends from the past hub. So it will expand the time and separation for retransmission. In the proposed Improved FTMR, not just the power level of hub will be analyzed dependably and furthermore the quality of the way in which it transmits the information or bundles. On the off chance that the getting hub's quality is recognized by transmitting hub and the power is nearing the edge level, then the transmission rate will be naturally lessened. It will locate a backup course of action and furthermore extra storing of bundles will be begun. But in this approach, it was only focused on time delay reduction not on other performance metric parameters. In the paper [9], proactive based fault-tolerant routing scheme was proposed for establishing reliable path and maintain the path among the mobile devices communication in heterogeneous environment. This scheme is a proactive based routing one which maintains updated information about the status of devices in the network. A MAC level communication and user interface identification was done during the time of broadcasting the message.

In addition to the mentioned characteristics, a Location based clustering and comparison based self-elimination methods were used in the selection of reliable and correct service provisioning nodes in the service path. The main issue was focused in this paper is fault tolerant was considered on only heterogeneous networks. The author of this paper [10],a blame tolerant

administration revelation convention was produced for MANET which works by making majorities of registry hubs, chose considering generally higher asset and lower portability and henceforth more dependable and less blame inclined. Keeping in mind the end goal to diminish benefit disclosure cost, the system was isolated into topological spaces, each served by some registry hubs. Here, administration enlistment and demand/answer are completed by spaces keeping in mind the end goal to lessen message cost and revelation delay. In addition, benefit data is imitated among the index majority individuals to deal with disappointments of specialist co-ops and catalog hubs and to guarantee arrange wide administration accessibility. The main issue of this paper is not focused on data availability if the packet was damaged or duplicated. In [11],learning automata based blame tolerant steering calculation (LAFTRA) was produced which is equipped for directing within the sight of defective hubs in MANETs utilizing multipath directing. Here they have utilized the hypothesis of Learning Automata (LA) for improving the determination of ways, decreasing the overhead in the system, and for finding out about the defective hubs exhibit in the system. The proposed calculation was assessed with existing steering convention in a MANET. In this approach, there is no mathematical proof was given for selecting optimized path in network.

In paper [13], it was presented that conveyed blame tolerant steering convention for QoS bolster in portable specially appointed systems, which mitigates interruption time under system failures. It was demonstrated that the customary technique for rerouting QoS activity from the source given a connection failure yields genuine negative QoS interruption results. An effective neighborhood blame tolerant calculation can essentially alleviate the time required to re-establish an association.

In paper [14], fully distributed cluster-based was proposed to progressive directing in that each bunch hub just keeps up QoS data for other group individuals, a small amount of the system. In this manner, an increase in hubs ought not altogether increase memory or runtime. Moreover, since worldwide system state is shared and kept up by all, the correspondence overhead is greatly reduced. In FDCB, if a stream's source and goal are not in a similar bunch, the source sends a course request parcel to the entryway hub, which advances it to neighboring group.

From the previous analysis, both clustering and multipath routing was deployed to improve the network lifetime. But they have not focused on network connectivity and fault tolerant rate. The main goal of our scheme is to strike the correct balance between organize network and blame tolerant rate.

3. Overview of Proposed Scheme

In the proposed Cluster based Multipath Fault tolerant routing, there are three phases involved namely Establishment of Multipath Routing, Cluster head selection and Fault Tolerant algorithm. In multipath routing, course disclosure

and course upkeep process are involved. Multipath routes are incorporated with proposed plan to avoid arrange failures, link failures and provide fault tolerance. In cluster head selection phase, each cluster member can elect a cluster head based on maximum residual power, mobility and high connectivity factor. In fault tolerant procedure, both the duplicate and original packets are calculated at the end of receiver. Cluster head maintains the fault tolerant table and routing table to keep track of network failure or any malfunctioning occurs in the network. The description of proposed scheme phases is given as below.

QoS based Multipath Steering Scheme

The principle point of proposed multipath directing is to discover different routes between cluster head to another cluster head. These numerous ways between source cluster and goal cluster sets can be utilized to make up for the dynamic and erratic nature of MANET, and bolster QoS. Multipath based directing conventions can find hub disjoint, connect disjoint, or non-disjoint courses. Hub disjoint courses, otherwise called absolutely disjoint courses, have no hubs or connections in like manner. Connect disjoint courses have no connections in like manner, however may have hubs in like manner. Non-disjoint courses may have bring down total assets than disjoint courses, in light of the fact that non-disjoint courses share connections or hubs.

1. Route Discovery Process

The procedure on each middle cluster member hub can be portrayed as takes after:

Step 1 If current hub itself is inside the Routing loop recorded by RREQ, it will dispose of the RREQ due to the steering loop. Something else, goto step 2;

Step 2 If the tuple (CH_ID, RREQ_ID) of RREQ is excluded in the steering table, which implies the present hub is the first run through to get this RREQ, it figures the relating estimation of the transfer speed. On the off chance that the esteem is not as much as Bmin, the RREQ will be disposed of. Something else, go to step 3;

Step 3 Append the estimation of data transfer capacity to the comparing fields of the RREQ. At that point the RREQ will be constantly sent. Go to step 1.

The goal node then sends a RREP for the chose RREQ. The procedure can be portrayed as takes after:

Step 1 Initialize the maximal number of courses N and Hmax;

Step 2 Calculate end-to-end unwavering quality as indicated by and sort the sequence(Routing_loop1, Routing_ loop2… Routing_loop n) in plunging request in view of the dependability values. Routing_loopi means the ith Routing_loop in the relating field in RREQ. RREQ recording with Routing_loop1 will be included into the reacting cradle;

Step 3 From Routing_loop2 to Routing_loopn, discover all Routing_loopi (i=2, 3… n) which disjoint with Routing_loop1 . On the off chance that the quantity of the multipath courses established is close to N and the bounces of each course is not as much as Hmax, the comparing RREQ will be included into the reacting cradle and the check of courses will be expanded by 1;

Step 4 If the emphasis completed or the directing number surpasses N, end the procedure. Something else, go to step3.

2. Routing Maintenance

While the source cluster member sending information along different courses, a few or the majority of the courses may break because of hub portability or connection and hub disappointments.

At that point course upkeep must be performed within the sight of course disappointments.

New course revelation can be set off each time when one of the courses comes up short or simply after every one of the courses fizzle. Moreover, because of the dynamic changes of assets, halfway hubs may have insufficient assets for the saving after they got RREP.

For the occasion, RERR message will be spread to the source hub for blunder preparing. In the period of mistake preparing, the hub which not able to meet the conditions for holding assets will send a disappointment message to the goal hub along the achievable way and discharges the assets officially saved.

Weight based Cluster Head Selection

In a given a random clustered topology of an Ad Hoc organize, nodes are adjusted with a minimum power level to get a well-connected network. The procedure to elect a cluster head is based on mobile node degree, transmission power of node, high connectivity factor, mobility and the packet receiving ratio of the hubs to choose bunch heads.

Each cluster member figures its aggregate weight as takes after:

$$AW_R = w_1\Delta_R + w_2 TP_R + w_3 C_R + w_4 M_R + w_5 PRR_R \quad (1)$$

factor Δ_R speaks to level of each hub R. Level of the hub is the number of neighbor cluster members of that node. It means that all cluster member hubs inside the transmission extend; *TPR* is transmission authority of nodes, C_R is the connectivity factor of cluster members. The running normal of the speed for each cluster member hub till current time τ gives a measure of portability and is meant by MR.

PRRR infers how much packets received at the destination with loss. In equation 1, the main segment, $w_1\Delta_R$, stays away from medium access control layer issues since it is constantly alluring for a group make a beeline for handle

up to a specific number of hubs. The second part is identified with transmission power since to convey for a more drawn out separation it requires more power. Subsequently, it would be better if the entirety of separations to all neighbor cluster members of a cluster head is less. The third segment is connectivity factor which describes maximum bandwidth of the cluster member node. The fourth segment, portability of the hub, a cluster head having less versatility demonstrates grater change towards solidness of cluster. Last part, PRRR, is the packet receiving ratio of a cluster member node. If this level is high, node can receive packets with high stability value.

Moreover, battery seepage will be more for cluster makes a beeline for cluster member nodes. The proposed cluster routing additionally gives the adaptability to alter the weighting elements as indicated by mobility of nodes and network requirements.

Step 1

At first each cluster member out of gear state and ascertains its aggregate weight AWR, then communicates their ids alongside AWR values. Once a hub got it, it checks for the hub with better AWR in its rundown and sets it as its cluster head and makes itself as cluster member.

Step 2

All hubs communicate their weights alongside ids in Hello message. Prior to each communicate; aggregate weight ought to be computed by each hub. At whatever point a cluster head got a communicate message from an un forwarded hub, it will answer with a Hello message quickly. In the wake of getting answer from a cluster head, the un forwarded hub changes heads while calculating an aggregate weight metric.

Step 3

If any node is chosen as cluster head, it checks for next best hub with better AWR among group individuals, and communicates it as auxiliary group make a beeline for group individuals.

In case if a bunch set out kicks the bucket toward some reason due to more packet loss, high battery drainage, optional group head takes obligations of essential bunch head and enhances the group steadiness by evading incessant link breakage of bunch development procedure.

Step 4

At the point when two bunch heads move alongside each other, then one of them will lose its group head position. i.e., at whatever point a bunch head gets a communicate message from another group head, it checks its own particular aggregate weight with that of the other bunch head's.

Step 5

On the off chance that any hub falls under the transmission scope of two group

heads, then the hub joins to the bunch, which having a bunch head with better aggregation weight (AWR). Each bunch is recognized by its group head id. Each hub keeps up information structures to store data about system.

Step 6

Each cluster member hub has two tables: Neighbor table and Fault tolerant table. Neighbor table contains the data of neighbor hub id and status, while fault tolerant table comprises of number of bundles dropped, number of parcels duplicated, number of unique parcels received. Additionally, there might be numerous passages to achieve neighbor cluster. The fault tolerant tables are refreshed intermittently by hi messages.

To pick up the Cluster Head (CHs), the following procedure is followed.

1. 1. ζ_w = get_minimum_ aggregate Weight
2. Q = cluster head
3. add neighbor cluster members of Q to vector ζ_w
4. REPEAT
5. σ_w = get_maximum_aggregate Weight in ζ_w
6. If σ_w covers new nodes
7. Q = cluster head
8. add neighbors of Q to vector σ_w
9. remove Q from vector σ_w
10. until network is covered.

Packet Delivery Approach

In the proposed packet delivery approach, the likelihood of the conveyance of parcels is efficiently estimated through the ways accessible at any minute. The proposed calculation consists of route evaluation stage and a route selection stage.

The route evaluation stage is utilized to appraise the parcel conveyance likelihood of the considerable number of routes at the transfer whenever moment, while the route selection stage is utilized to choose those routes. Both route evaluation and route selection phases are affirmed to have fulfilled a specific improvement control, and to drop the superfluous multipath routes between a couple of cluster head to another cluster head sets. In the proposed strategy, the bundle conveyance likelihood estimation is refined with the expansion in the quantity of cycles.

In each emphasis, an arrangement of bundles is transmitted through each of the multipath routes between a couple of source cluster head-goal cluster heads. There are two conceivable situations for any way i.e. the hubs in a way either forward the bundles effectively, or they don't. The following algorithm is developed for fault tolerant based routing against network failures, link failures

and misbehaving nodes.

Algorithm:

Input

- A system model with an arrangement of cluster member hubs, and an arrangement of multipath associating the hubs.
- Mobile hubs and paths are interfacing with the adjustment in the position of the hubs.
- Due to misbehaving hubs in the system, a few hubs are flawed with a specific bundle conveyance rate reliant on the separation of the hub.

Output

- All the approaching bundles are conveyed from the cluster head to another cluster head, with the goal of augmenting the parcel conveyance rate, limiting the system overhead and power level.

Procedures

BEGIN

Step 1:

Introduce a vector CBMR_ RP that stores every one of the ways being used, and CBMR_cluster members that stores every one of the hubs in the chart, alongside the data about their assessed parcel conveyance probabilities.

Step 2:

Spare the evaluated bundle conveyance likelihood of every hub in the vector CBMR_cluster members.

Step 3:

Refresh the edges and probabilities in the chart to mirror the present position of the cluster member hubs, and figure the new ways from the cluster head to neighbor cluster head.

Step 4:

Utilize the qualities put away in CBMR_Cluster Member to compute the assessed parcel conveyance likelihood of every way.

Step 5:

Attempt to affirm or drop ways. Ways dropped are expelled from the CBMR_ RP vector.

Step 6:

Use every one of the ways in the CBMR_RP vector to send the bundles, and compute the quantity of parcels that are gotten for every way and the aggregate number of non-copied parcels that are gotten.

END

Fault Tolerant based Route Power Determination

In CMFTRS, hubs that are not on a chosen way don't keep up directing data or take part in steering table trades.

The course disclosure of the CMFTRS is as per the following.

Step1:

At the point when the source hub needs to make an impression on the goal hub and does not as of now have a substantial course to that goal, it starts a way revelation procedure to find the other hub. The source hub scatters a course ask for (RREQ) to its neighbors. The RREQ incorporates such data as goal Internet ID, control limit (the base vitality of all hubs in the present discovered course), goal grouping number, jump check, lifetime, Message Authentication Code (MAC) is for giving testament expert to the hubs and Cyclic Redundancy Code (CRC) for blunder recognition and amendment. The goal arrangement number field in the RREQ message is the last-known goal succession number for this goal and is duplicated from the goal grouping number field in the steering table. On the off chance that no arrangement number is known, the obscure grouping number banner must be set. The power limit is equivalent to the source's vitality. The bounce tally field is set to zero. At the point when the neighbor hub gets the parcel, it will forward the bundle in the event that it matches.

Step 2:

At the point when a hub gets the RREQ from its neighbors, it first expands the bounce include esteem the RREQ by one, to represent the new jump through the middle of the road hub. The maker grouping number contained in the RREQ must be contrasted with the comparing goal succession number in the course table passage. In the event that the maker grouping number of the RREQ is at least the current esteem, the hub thinks about the power limit contained in the RREQ to its present vitality to get the base. On the off chance that the maker grouping number contained in the RREQ is more prominent than the current incentive in its course table, the hand-off hub makes another section with the arrangement number of the RREQ If the maker succession number contained in the RREQ is equivalent to the current incentive in its course table, the power limit of the RREQ must be contrasted with the relating power limit in the course table passage. On the off chance that the power limit contained in the RREQ is more noteworthy than the power limit in the course table section, the hub refreshes the passage with the data contained in the RREQ.

Amid the way toward sending the RREQ, middle of the road hubs record in their course tables the locations of neighbors from which the primary duplicate of the communicate bundle was gotten, so building up a hold way. On the off chance that the same RREQs are later gotten, these bundles are quietly disposed of.

Step 3:

Once the RREQ has touched base at the goal hub or a middle of the road hub with a dynamic course to the goal, the goal or moderate hub produces a course answer (RREP) bundle. In the event that the creating hub is a middle of the road hub, it has a dynamic course to the goal; the goal grouping number in the hub's current course table passage for the goal is at least the goal succession number

of the RREQ. On the off chance that the producing hub is simply the goal, it must refresh its own succession number to the most extreme of its present arrangement number and the goal grouping number in the RREQ parcel quickly. While producing a RREP message, a hub spreads the goal IP address, maker grouping number, and power limit from the RREQ message into the comparing fields in the RREP message.

Step 4:

At the point when a hub gets the RREP from its neighbors, it first builds the bounce include esteem the RREP by one like,

Jump number = Hop check +1

At the point when the RREP achieves the source, the jump number speaks to the separation, in bounces, of the goal hub from the source hub. The maker succession number encased in the RREP must be contrasted with the relating goal arrangement number in the course table section. On the off chance that the originator succession number of the RREP is at the very least the current esteem, the hub thinks about the power limit contained in the RREP to its present vitality to get the base, and after that updates the power limit of the RREP with the base. The power limit field in the course table section is defined to the power limit contained in the RREP.

Proposed Bundle Design

The Proposed bundle design of CMFTRS is given below.

Cluster head ID	Net. Conn. Status	Seq. Num.	Agg. Weight	MAC	FCS	CRC

Figure 1: Proposed Bundle Design

In fig.1, the bundled design of proposed scheme is exposed. Now the initial field occupies 4 bytes where ID of cluster head is monitored by cluster member nodes. The second field is Network connectivity status which occupies 4 bytes. In next field, Sequence number is maintained by each cluster head and its cluster members. It occupies 1 byte. In fourth field, aggregation weight occupies 3 bytes which is used to choose the cluster head. MAC is for message authentication purpose. It occupies 2 bytes. Remaining two fields are frame check sequence and cyclic repetition check. Both occupy 2byte field for blunder detection and correction.

4. Performance Evaluation

Simulation Model and Parameters

Our proposed CMFTRS is implemented with the network simulator tool (NS2.34). In this simulation, 200 portable hubs move in a 1200 meter x 1200 meter square district for 100 seconds re-enactment time. We expect every hub moves freely with a similar normal speed. All hubs have a similar transmission

scope of 250 meters. The re-enacted movement is Constant Bit Rate (CBR).

Our reproduction settings and parameters are condensed in table 1.

No. of Nodes	200
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	100 sec
Transmission Range	250 meters
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point

Performance Metrics

We assess primarily the execution as indicated by the accompanying measurements.

Bundle Delivery Ratio: It is the proportion of the quantity of parcels got effectively to the aggregate number of bundles transmitted.

Computation Overhead: The control overhead is characterized as the aggregate number of directing control parcels standardized by the aggregate number of got information bundles.

In **end-to-end delay**, a parcel relies on upon the directing disclosure dormancy, extra postponements at each jump and number of bounces.

Availability Ratio: It is characterized as the proportion of number of connections associated between the hubs to aggregate connections over the system.

Probability of network failure proportion: It is determined as the probability of number of path failures to aggregate paths set up between portable hubs.

Data availability Ratio: It is the proportion of total facts available to target node and entire numeral of nodes available.

Network lifetime: It is defined as maximum residual energy of node to total energy of nodes.

Result

We compared our proposed scheme CMFTRS with EFDCB [13] and FDCB [14]. The outcomes are inspected by utilizing execution measurements end-to-end delay, parcel conveyance ratio, probability of network failure ratio, end to end postpone and overhead. Fig.4 demonstrates the examination of Speed Vs Packet Delivery Ratio. From the outcomes, our proposed conspire accomplishes

high parcel conveyance ratio than the current scheme FDCB. In fig.2, we differ the simulation time as of 5 to 25secs.While+ expanding the simulation time, the network proportion of proposed calculation CMFTRS is higher than EFDCB and FDCB. In this analysis, movement of the nodes is increased rapidly. Initially, the proposed scheme CMFTRS achieves 98% packet delivery ratio, after that it gets decreases. Because when the mobility increases, node may move out of region, so the communication between cluster head and cluster members may by slightly suppresses. Packet delivery ratio gets decreased. But compared to previous approach, proposed scheme achieves high delivery ratio. Because of fault tolerant routing, network can be capable of handling all route failures. So the communication between the nodes can be improved by means of increased parcel conveyance proportion. In fig.2, the CMFTRS achieve slow end to end defer than EFDCB and FDCB. The proposed scheme achieves0.28-0.14 delay than the previous conspire. If the delay increases, congestion rate will decrease. In route selection method, best routes are chosen based on packet delivery rate. If the route has high packet delivery rate means, packet loss is less. Several approaches are not focused on delay. In our approach, end to end postpone of bundles is reduced by means of reducing packet intervals. In previous work EFDCB and FDCB, end to end postpone is not greatly concentrated in route maintenance process. Due to the implementation of multipath routing, the proposed scheme achieves low end to end delay. Fault tolerant adopt aggregate weights to choose the cluster head. Cluster heads forward the packet through selected minimum energy consumption path. Delay between the nodes will get decreased.

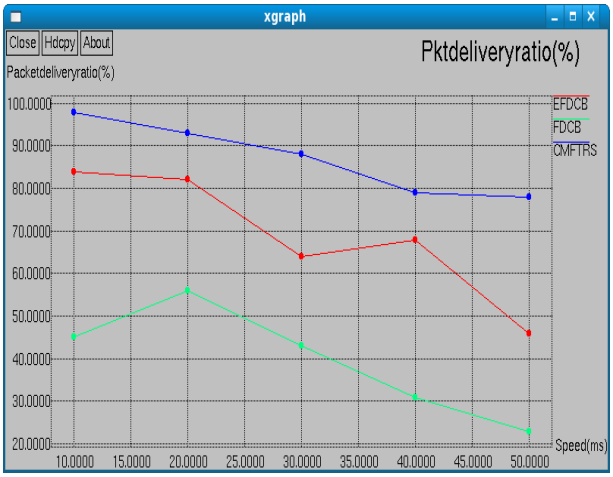

Figure 2: Speed Vs Packet Delivery Ratio

In fig. 3 we differentiate the number of nodes like 5, 10,…50. The probability of network failure ratio of CMFTRS achieve lower than EFDCB and FDCB. In this analysis, network gets full connected and communication between the clusters increased. This will lead to decreased network failure ratio of proposed scheme CMFTRS. In previous work, no focusing on aggregate weight for the

selection of cluster head, so network performance is getting degraded. In our scheme we have implemented to reduce the network failure rate. When the number of nodes increased, nodes get disconnected because of dynamic topology. But the cluster member's status is always updated to cluster head. So cluster head determines best route to reduce network failure ratio.

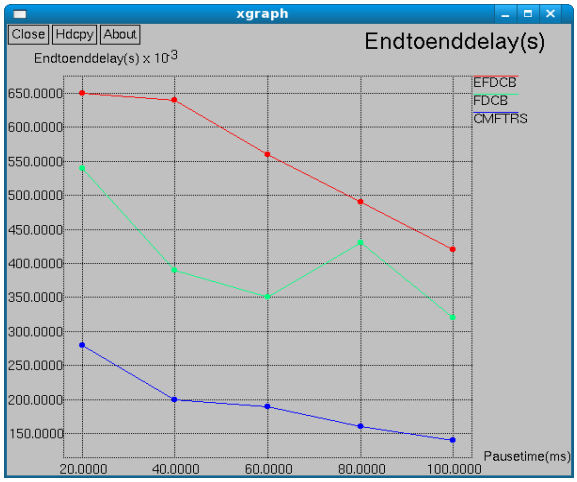

Figure 3: Pause Time Vs End to End Delay

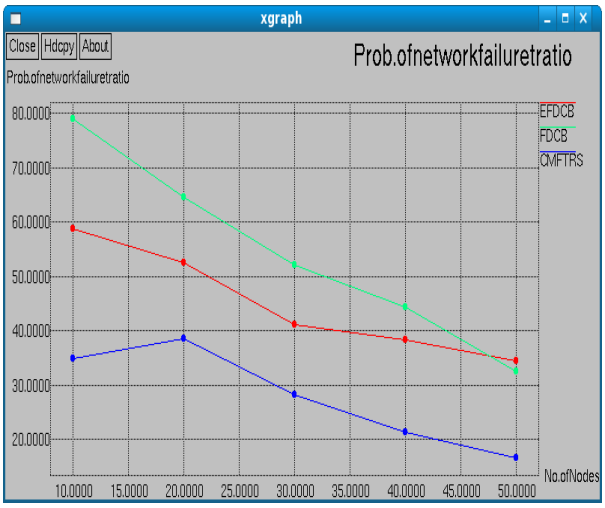

Figure 4: Probability of Network Failure Ratio Vs No. of Nodes

In fig.4, nodes are differentiated as 10, 20….200. When we increment the number of nodes, the computation overhead is also getting decreased. The proposed calculation CMFTRS has low over head per parcel than the current steering schemes like EFDCB and FDCB. Computation overhead implies that more data control packets. In cluster regions, cluster heads are responsible for monitoring the behavior of cluster members. So the probability of overhead

occurrence is low. Cluster heads only forward the more data packets while sending less control packets. So the overhead will be low. The proposed scheme CMFTRS achieves less computation overhead than previous schemes.

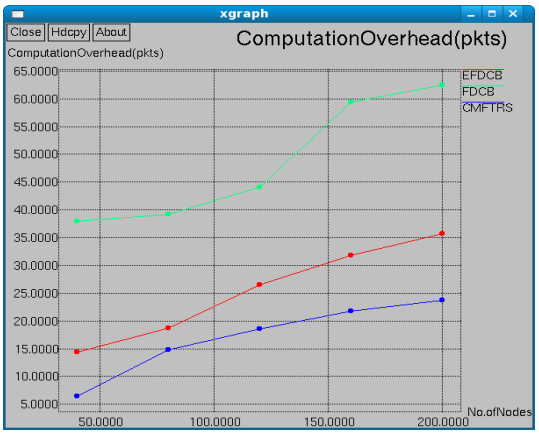

Figure 5: Number of Nodes Vs Computation Overhead

In fig.5, simulation time is varied as 5, 10….25secs. The availability proportion of the proposed calculation CMFTRS is superior than the current routing scheme EFDCB and FDCB. Misbehaving nodes are isolated from the fault tolerant route in the proposed plot. Route selection process is implemented in our approach to overcome the effect of misbehaving nodes. In previous scheme, lack of misbehaving nodes is identified. This will lead to high network connectivity ratio. Simulation time increases connectivity ratio of the CMFTRS.

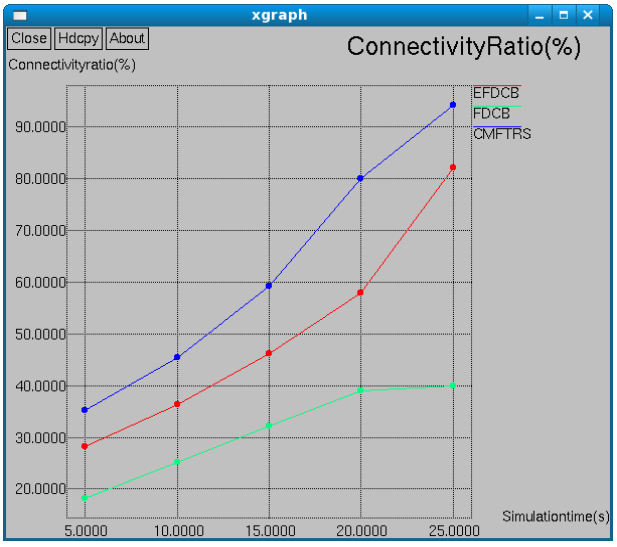

Figure 6: Simulation time Vs Network Connectivity Ratio

In fig.6 mobility is varied as 20, 40…100secs. Compared to EFDCB and FDCB scheme, the proposed CMFTRS achieves higher fault tolerant because of fault tolerant based routing.

Fault tolerant is determined how well the network can be capable of tackle the route failures and node failures. Based on isolated misbehaving nodes, fault tolerant is getting increased.

In fault tolerance routing, initialize vector is chosen based on route selection and route evaluation method.

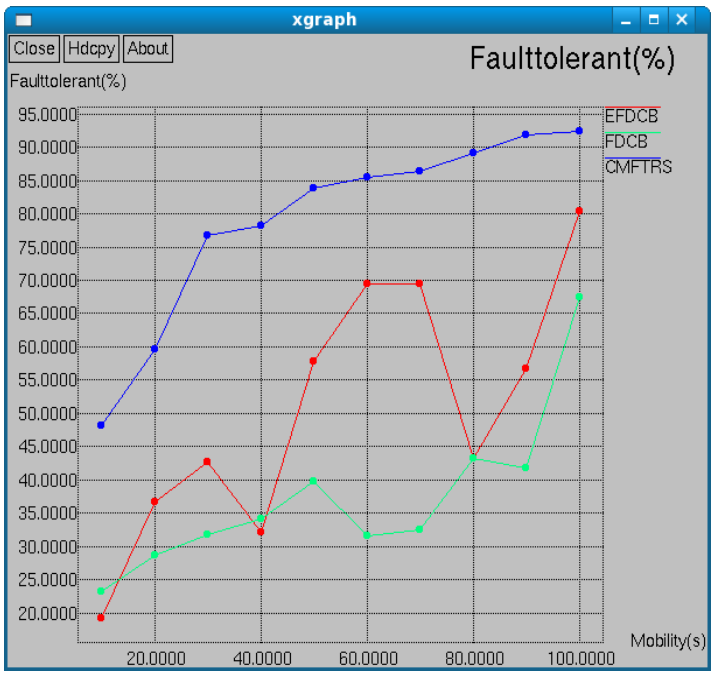

Figure 7: Mobility Vs Fault Tolerant Rate

In fig.7, simulation time is varied as 10, 20…50 ms. When we increase the time, the data availability ratio is increased.

The proposed algorithm CMFTRS has high ratio per packet than the existing routing schemes like EFDCB and FDCB.

Data availability ratio of CMFTRS is higher than previous scheme. It is because of cluster with adaptive fault tolerant routing.

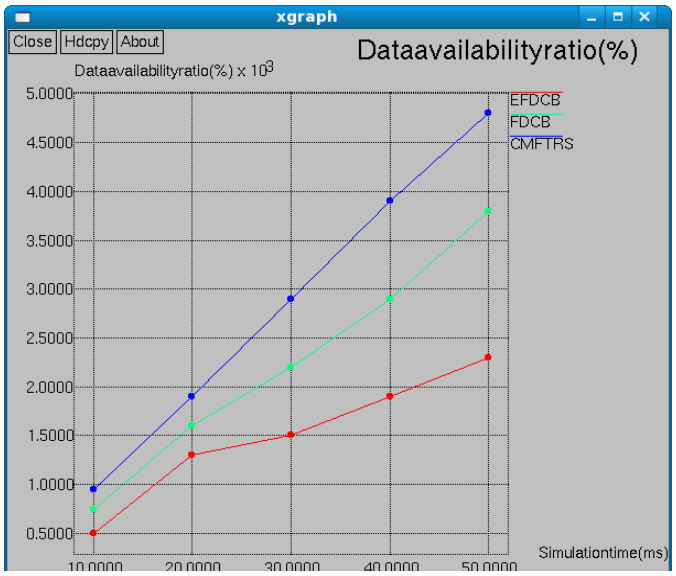

Figure 8: Simulation Time Vs Data Availability Ratio

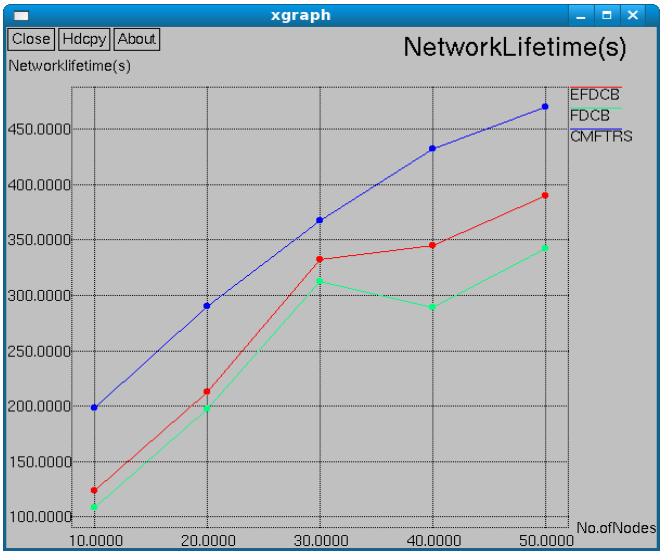

Figure 9: Number of Nodes Vs Network Lifetime

In fig. 8, 9 number of hubs is differed as 5, 10….50. The network lifetime of the proposed algorithm CMFTRS is higher than the existing routing scheme EFDCB and FDCB. While energy consumption minimizes, the network lifetime gets increased. If more number of nodes increases, connectivity ratio of proposed scheme increases which also increases the network lifetime.

Table 2: Analysis of Proposed Method and Existing Methods in Terms of Different Parameters

Metrics	CMFTRS	FDCB	EFDCB
Probability of network failure ratio	34.89-16.55	78.89-32.55	58.89-34.55
Delivery ratio (%)	98-78	45-23	84-46
Network Lifetime (secs)	198.45-469.89	108.45-341.89	123.45-389.89
End to end delay (msec)	0.28-0.14	0.54-0.32	0.65-0.42
Overhead	6.45-23.67	37.89-62.45	14.45-35.67
Fault tolerant Rate	48.2-92.4	23.2-67.4	19.2-80.4
Data Availability	950-4800	750-3800	500-2300
Network Connectivity Ratio	35.232-94.123	18.22-39.99	28.23-82.12

5. Conclusion

From the previous analysis, lack of balancing between network connectivity and fault tolerant rate. In our proposed scheme, we have achieved high fault tolerance rate using multipath fault tolerant routing. Cluster heads are communicated through fault tolerant paths which against node failures and network failures. We have simulated our proposed scheme regarding overhead, system connectivity ratio, parcel conveyance extent, network failure ratio furthermore, end to end delay. In future, we plan to actualize cluster enhanced secure checkpoint in mobile distributed computing systems. In this scheme we plan to develop optimized signature generation and verification scheme.

References

[1] Swati Saxena, Madhavi Sinha, Single-Response Metric Analysis of Adaptive Fault Tolerant Replication Routing Protocol for MANETs using Taguchi Approach, International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) 3 (3) (2013), 105-116.

[2] Ajay Agarwal, QoS-constrained Fault-tolerant Routing in MANETs based on Segment-Backup Paths, IEEE Conference on Communication System Software and Middleware, Comsware (2006), 1-9.

[3] Ahamed A.A., Kumar M.A., Shivakumar B.L., Secured Data Forwarding Routing Protocol (SDFRP) For Heterogeneous Mobile Ad Hoc Networks, International Journal of Computer Trends and Technology (IJCTT) 39 (1) (2016).

[4] Eyuphan Bulut Boleslaw K.S., Friendship Based Routing in Delay Tolerant Mobile Social Networks, IEEE Conference on Global Communication (2010), 1-5.

[5] Arvindh G.V., Kumar R.P., Fully Distributed Cluster based Fault Tolerant Service, In International Conference on Computing and Control Engineering (ICCCE 2012) (2012), 1-3.

[6] Patil R., Shah S.R., Cross layer based virtual node layer for reactive MANET routing, International Journal of Engineering Research & Technology 1 (6) (2012), 1-7.

[7] Li Z., Wang H., A adaptive based routing for MANET, In 11th Joint International Conference on Information Sciences, Atlantis Press (2008), 1-6.

[8] Rajkumar G., Duraiswamy K., Time Delay Reduction in MANETs using Improved Fault Tolerant Routing Protocol, CARE Journal of Applied Research (2014), 1-3.

[9] Shaji R.S., Rajesh R.S., Ramakrishnan B., A Fault-tolerant scheme for Routing Path Reestablishment for reliable communication in Heterogeneous Networks, International Journal of Scientific & Engineering Research 1 (3) (2010), 1-10.

[10] Vaskar Raychoudhury, Efficient and Fault Tolerant service Discovery in MANET using Quorum-based Selective Replication, IEEE International Conference on Pervasive Computing and Communications (2009), 1-2.

[11] Sudip Misra P., Venkata Krishna, Akhil Bhiwal, Amardeep Singh Chawla, Bernd E.W., Changhoon Lee, A learning automata-based fault-tolerant routing algorithm for mobile ad hoc networks, Journal of Supercomputing 62 (1) (2012), 4-23.

[12] Hoai Phong Ngo, Myung Kyun Kim, MRFR - Multipath-based Routing Protocol with Fast-Recovery of Failures on MANETs, KSII Transactions On Internet And Information Systems 6 (12) (2012), 3081-3099.

[13] Larry C.L., Kenneth M.H., Scott R.G., Distributed Fault-Tolerant Quality of Wireless Networks, IEEE Transactions on Mobile Computing 10 (2) (2011), 175-190.

[14] Ahamed A., Shivakumar B.L., A Survey on DSDV Node Design in Wireless Ad Hoc Networks, International Journal of Advanced Research in Computer Science 6 (8) (2015), 65-69.

[15] Thamrin A.H., Kusumoto H., Murai J., Scaling Multicast Communications by Tracking Feedback Sensors, Proceedings of International Conference on Advanced Information Networking and Applications (AINA) (2006), 1-6.

[16] RAJESH, M. "A SYSTEMATIC REVIEW OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATION." The Online Journal of Distance Education and e- Learning 5.4 (2017): 1.

[17] Rajesh, M., and J. M. Gnanasekar. "Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation." Computer Engineering and Intelligent Systems 6.8: 24-26.

[18] Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous WANET using FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974 (2015): 2115.

[19] Rajesh, M., and J. M. Gnanasekar. "Hop-by-hop Channel-Alert Routing to Congestion Control in Wireless Sensor Networks." Control Theory and Informatics 5.4 (2015): 1-11.

[20] Rajesh, M., and J. M. Gnanasekar. "Multiple-Client Information Administration via Forceful Database Prototype Design (FDPD)." IJRESTS 1.1 (2015): 1-6.

[21] Rajesh, M. "Control Plan transmit to Congestion Control for AdHoc Networks." Universal Journal of Management & Information Technology (UJMIT) 1 (2016): 8-11.

[22] Rajesh, M., and J. M. Gnanasekar. "Consistently neighbor detection for MANET." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.