ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Position Aided Cluster Based Routing for Extending Manet Lifetime.

Kavitha T*, and Muthaiah R.

School of Computing, SASTRA University, Thanjavur, Tamilnadu, India.

ABSTRACT

One of the major drawbacks in Mobile Ad-hoc Networks routing protocols is that, many essential conditions such as load balancing, network lifetime improvement and security are not covered all together. Though efficient routes can be obtained with high transmission hit rate by using on-demand routing protocols, balancing of load on each node along with their security is not considered. This may cause instability in the network. Thereby, we propose a new protocol, Position Aided Cluster based Routing, which solves all the constraints related to the above mentioned essentialities of a mobile ad-hoc network. The traditional ad-hoc paradigm is slightly changed by adding a Route Computation Unit, which gives a shorter, secured and load balanced pathway on request. All possible circumstances are taken into consideration. The appropriate and operational solutions are provided. The simulation results prove that our methodology has a greater enhancement in network lifetime and facilitates message transmission with balanced load on each nodes. It is also observed that a node with very low energy sustains in the network for a longer period of time.

Keywords: MANET Lifetime, Load Balancing, Clustering, Position Aided Routing.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

With tremendous development in the fields of mobile computation and networking, the applications of mobile ad-hoc networks (MANET) are widening day by day. MANETs are temporary networks formed with dynamism by a gathering of arbitrarily sited wireless nodes that are in motion irrespective of direction. Its initial objective was to facilitate communication between nodes during emergency situation and war field. Later its track has been diversified to facilitate various day to day services in the fields of communication, mobile applications, transportation, entertainment, etc. There are lot of protocols such as DSDV [1], AODV [2], DSR[3], ZRP [4], OLSR [5], AOMDV[6] etc., each with their own merits and demerits. Not all essentialities are taken into account by these protocols and some are even sacrificed. Due to mobile nature of nodes, their position may vary dynamically with time. This causes change in neighbors of a node. Therefore we require a position based routing at the time of communication initiation which is provided by reactive routing methodologies. The need to perform load balancing [7] is to avoid repeated transmission through the same node.

The objective of our proposed methodology is to obtain a shorter, secured and load balanced route for message transmission. The role of Route Computation Unit (RCU) is to improve the network lifetime by choosing a secured and load balanced path for message transmission between the Communication Initiator (CI) and Communication Beneficiary (CB). In case of link failure [8], the RCU helps to identify a new route and rebuilds the network. The lifetime of the network is sustained by implementing security measures from base level. The concept of clustering [9] [10], is used to group the mobile nodes into temporary clusters which are continuously monitored by their respective cluster heads. This kind of networks can be implemented in disaster scenario [11] and military applications [12].

The rest of the paper is organized as follows: Section 2 discusses the load balancing techniques in various methodologies. Section 3 describes the working of our methodology under various circumstances. Section 4 validates our methodology with the help of simulated results followed by conclusion in Section 5.

RELATED WORK

The major setback in using Fibonacci protocol [13] is that, shortest path selected is used more frequently than the other ones. Due to this, there is a certain chance for the node to get exhausted. Also the paper proposes a multipath technique to increase the transmission hit rate thereby reducing the congestion [14], but this may not be the case every time. Once the nodes of the shortest path tend to fade away, the problem of congestion arises. Here the security parameters of the network are very weak and any malicious node can be a part of it. AOMDV suggests routing through multiple pathways. The major setback in this protocol is the involvement of nodes irrespective of their energy level for a message transmission in case of very few neighboring nodes. Another major defect is the delay in transmission of data packets due to the interference of disjoint nodes. Also the security parameter is another factor of concern. In the multi-cast routing protocol [15], the energy of each node is affected. This protocol mainly focuses on the transmission hit rate and decreasing the congestion. But for a network to be stable, these conditions are not sufficient. Also the load balancing is very acute and hence the network may collapse anytime. The security of the network is the least of concerns in this approach. In fuzzy mechanism [16] the major parameters are considered to be hop count, traffic load of gateway, and variance in receiving intervals of the gateways. Hence there will be a greater loss in packets if the load at the gateways is going to be higher. The security of the network is not maintained due to a major focus on the load balancing. In ANFIS [17], and SWARM [18] the setback is the usage of an agent driven routing technique. The agent based routing is prone to threats and hence the security of the agent is a major drawback. It fails once malicious node acts as an agent there by collapsing the entire network. The agent driven method is an ideal way of load balancing but it can act only on specific node for a period of time. But due to the usage of multicast routing protocol here the nodes use more amount of energy to perform a transmission as multiple data packets are copied to different nodes. Hence objective of this paper is not fulfilled. In case of multipath routing protocols [19], the same problem of the multi-cast occurs here. The only difference between them is that in multi-cast, the packet is sent through all the available routes to the destination, whereas in case of multi path it checks for multiple paths, and uses one among them. The major setbacks of this protocol are transmission delay, insufficiency in bandwidth and security measures. The mobility prediction based protocol [20] provides a solution to the link failure problem by using the expected

ISSN: 0975-8585

region concept. The setback of this protocol is that the nodes have to decide whether to forward the data packet based on certain parameters which is the additional computational load on the nodes thereby resulting in delay of transmission.

PROPOSED SOLUTION

Experimental Setup

The proposed methodology is a hybrid architecture for MANET (Fig. 1) that uses a tamper proof and non-exhaustive RCU with high storage, computational speed and transmission range. The RCU contains a list of nodes that are pre- registered to participate in the network. If any new node tries to connect to the network without registering with RCU, it is considered as a malicious node. Another role of RCU is to provide a shorter, secure and load balanced route between CI and CB. The type of nodes considered are laptops, mobile phones, PDAs that can recognize their position using GPS and has the capacity to participate in the network actively while they are in motion. The energy level of each node in the network is considered in two levels. They are,

E_n (t) - Energy of node n at time t (1)
E_{TH} (n) - Threshold energy of node n (2)

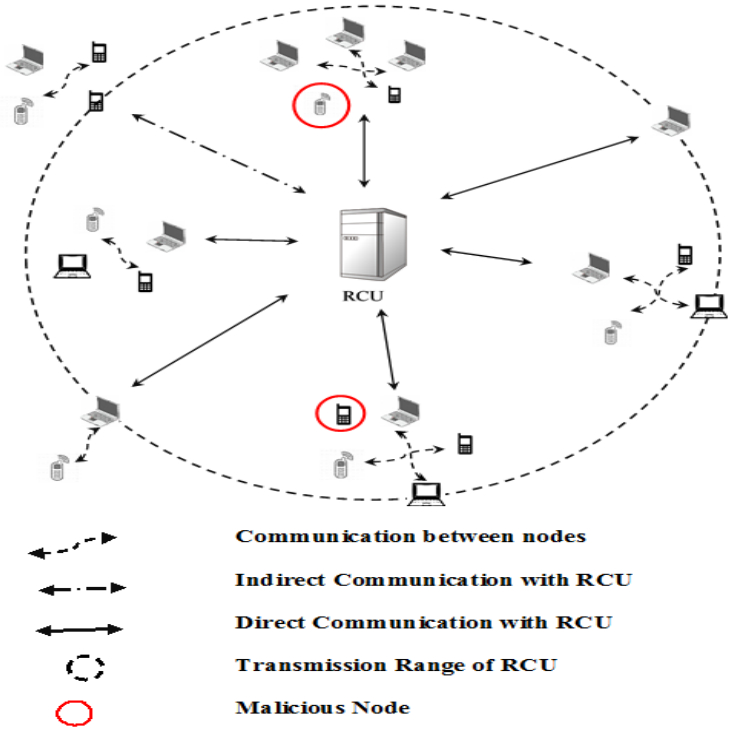

Fig. 1 Hybrid Architecture of MANET with RCU

The threshold energy E_{TH} represents the minimum energy required for functioning of the node. Each node's position $P_n(t) = (\alpha_t, \beta_t)$ and velocity are updated periodically. The displacement of node n during the time interval $(t - t_0)$ can be calculated using equation (3).

$$y_n = \sqrt{(\alpha_t - \alpha_0)^2 + (\beta_t - \beta_0)^2} \quad (3)$$

where, (α_t, β_t) is the position of the node at time t, (α_0, β_0) is the position of node at an earlier time t_0, y_n is the displacement of node n from time t_0 to t. Using equation (3) we calculate the velocity $V_n(t)$ of a node n at time t as,

$$V_n(t) = \frac{y_n}{t - t_0} \quad (4)$$

ISSN: 0975-8585

Cluster Formation

When more than one node comes within the proximity of the each other, the cluster formation begins and cluster head election takes place. Cluster head is the node which satisfies the criteria of having higher energy, least mobility and higher security credentials. The other nodes within the proximity of the cluster head act as its members. The node will function as a cluster head until its energy level comes down to the threshold energy (E_{TH}). Whenever a cluster head gets elected, its threshold energy is increased so that once the cluster head gets exhausted, it will have minimum energy to continue in the network as a normal node. The cluster head accepts a node based on a security check which involves verifying the new node ID with the pre-registered node list of RCU. If authenticated, the new node is added to its member table. The cluster head assigns its own ID as the master ID for the new node. The clustering under various situations is depicted in Fig. 2.

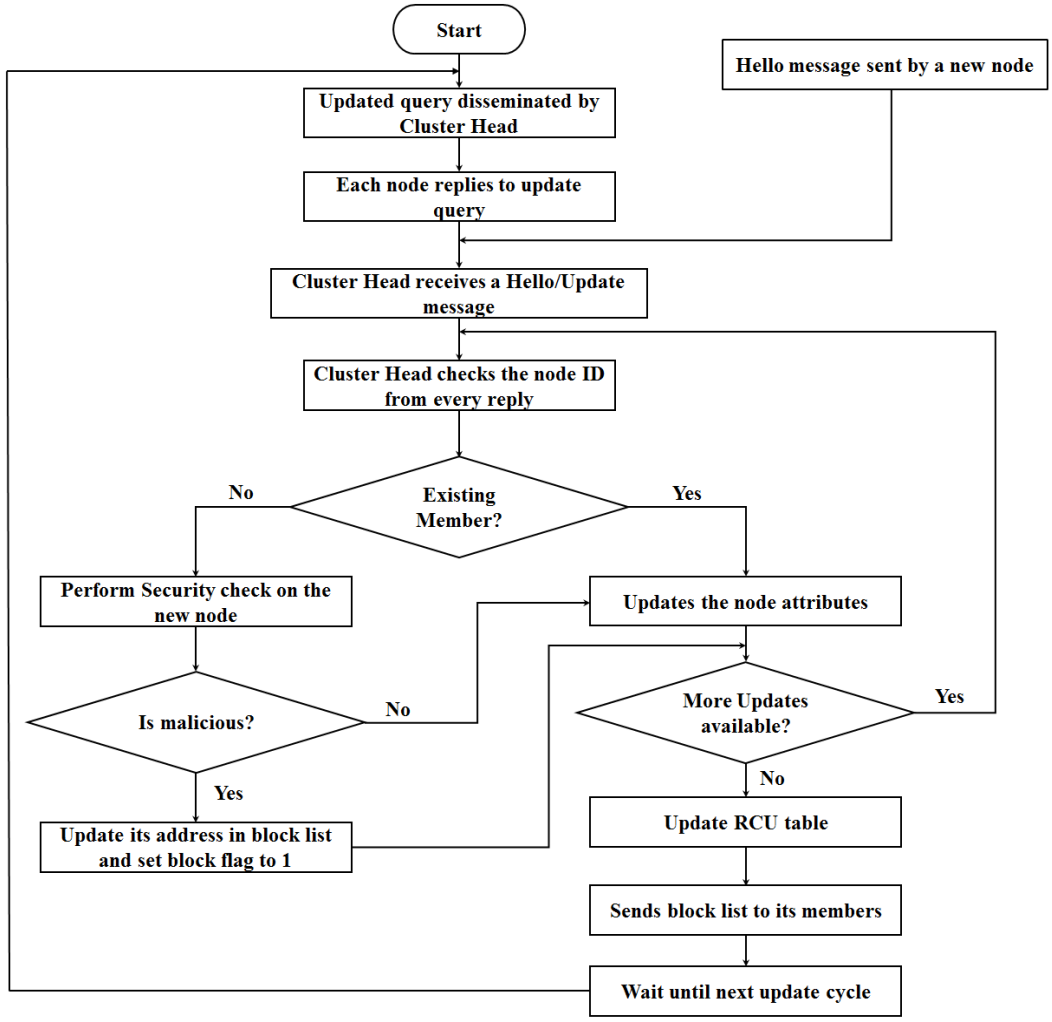

Fig. 2 Process of Cluster Head Update Cycle

Clustering Scenarios

Case 1: New Node Entry

When a new node comes into proximity of the cluster head, it has to register itself to the cluster head for working as its member. This is done as follows: The new node disseminates a hello message (Fig. 3a) to the cluster. The cluster head checks the security credentials of the new node. If the node is authenticated, it replies to the hello message by sending an acknowledgement (Fig. 3b) to it. The new node's position,

ISSN: 0975-8585

velocity, energy level, threshold value and block flag (0 for genuine node) are updated in its member table and in RCU (during periodical update) (Fig. 3c). If the security credentials are not fulfilled, then the cluster head sets the block flag (block flag =1) for that node ID. The cluster head informs its members about the presence of malicious node by sending the malicious update packet (Fig.3d). Upon receiving this message, the member nodes update their block list with the new blocked node's ID.

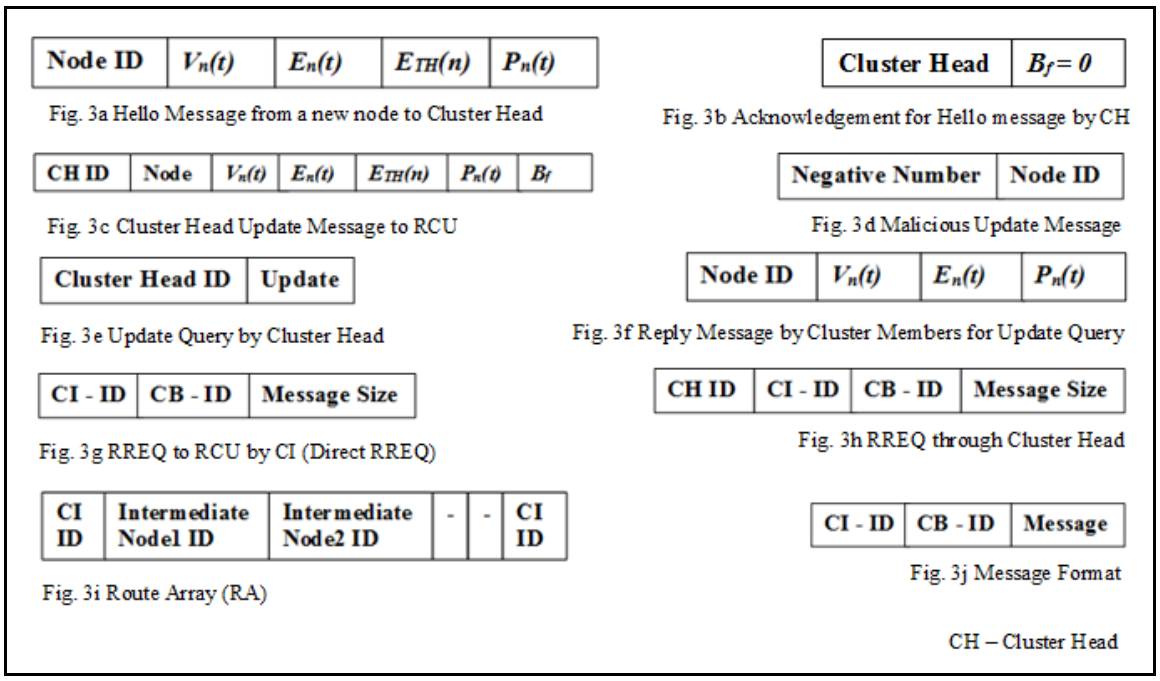

Fig. 3 Control Message Packets

Case 2: Position update

Based on the average velocity of the cluster, cluster head updates the position of its members at regular time intervals T_{avg} (equation 6). The cluster head disseminates the update query (Fig.3e) by the end of these time intervals. Upon receiving the replies (Fig. 3f) from its members, the cluster head updates their current position, velocity and the energy level in its member table and later updates the RCU.

$$V_{avg} = \frac{\sum_{i=2}^{n} v_i}{n} \quad (5)$$

$$T_{avg} = \frac{V_{avg} R_{tr}}{2} \quad (6)$$

where, T_{avg} is the update time interval, V_{avg} is the average velocity of a cluster, R_{tr} is the transmission range of the respective cluster head.

Case 3: New Member Update

During the position update cycle, if there exists any new member, its identity is verified with the RCU. If the node is authenticated then its attributes are registered with its new cluster head's member table and the RCU. If the security credentials are not fulfilled then the block flag is set to 1 for the respective node. The cluster head sends a malicious update packet to its members and updates its own block list with the new node ID. The algorithm for position update by cluster head is provided in Table 1.

ISSN: 0975-8585

Table 1 Algorithm for position update by cluster head.

Nomenclature: N_i is the i^{th} Node, M_t is the Member table of the respective cluster head and $B_{f(i)}$ is the Block flag for i^{th} node.
Begin
For (N_i : N_i within the proximity of Cluster head)
Check if $N_i \in M_t$
Update M_t
Else in case of new node
Increment Member list size by 1;
Add N_i to M_t
Set $B_{f(i)}$ based on the security credentials of (N_i);
If ($B_{f(i)}$ is true)
Add N_i to block list and update its attributes
End if
End if
End loop
Send update message to RCU.
Send block list update message to all members of cluster.
End

Case 4: More than one cluster head in each other's proximity

When more than one cluster head comes within the proximity of each other, the cluster head election takes place. The best node is chosen amongst them based on their energy level and stability. The new cluster head sends an acknowledgement packet to all its authenticated members followed by an update query (Fig.3e) to check through its members once again. The member table is communicated to RCU with new master ID.

Case 5: Exhausted Cluster Head

Once the energy of a cluster head comes down to E_{TH} (equation 2), it chooses the best node within its member table as the new cluster head. The member table of old cluster head is transferred to the new cluster head. The members are updated with the new master ID which in turns updated in the RCU table.

Case 6: Disjoint Node Case

Whenever a node comes out of a cluster and remains disjoint, i.e., not under the proximity of any other cluster, it can form its own cluster and remain as the cluster head. The RCU can check the authenticity of this node in its table and if found to be insecure, it rejects the cluster.

Case 7: Cluster Head is not within the proximity of RCU

When the cluster head is not under the proximity of the RCU then, cluster head sends the update to RCU using AODV routing protocol with the help of other cluster heads.

Route Computation Unit (RCU)

The objective of the RCU is to provide a shorter, secure and load balanced route for CI towards CB.

This is calculated using the data from RCU table (Table 2) and Position Aided Cluster based Routing (PACR). In addition to the route computing facility, it also consists of a list of registered nodes that are participating in the network. This list is used to authenticate the members of the network. The RCU table is updated periodically at T_{avg} in equation (5) time by every cluster head (Fig. 3c) in the network, which makes its data highly accurate. This RCU table is utilized efficiently by the PACR algorithm (Section 3.3.2) for computing shorter, secured and load balanced paths for node to node communications in the network.

Table 2 List of RCU table parameters.

Node ID
Cluster ID
Master ID
Velocity of the Node
Threshold Energy
Current Energy
Block Flag

Route Discovery

Whenever there is a need to perform an inter and intra cluster communication between nodes which are not in proximity of each other, a Route Request (RREQ) is sent by the CI to RCU directly(Fig. 3g) or through cluster head (Fig. 3h) . Once the RREQ is sent, the CI continues with its internal tasks until it receives the requested route in the form of a Route Array (RA) from the RCU. The computation of RA is done by RCU using the PACR algorithm.

Position Aided Cluster based Routing Algorithm (PACR)

The PACR algorithm is explained with a sample network which is shown Fig.4a. Once the RREQ from a node (CI) is received by the RCU it checks for the authenticity of CI and CB. This is done by checking the block flag for the respective nodes in the RCU Table. If either one is blocked, the request is discarded. If not, CI is set to source. First, the source is added to Route Array (RA). The required attributes for route computation such as the nodes position, current energy, threshold energy, status of block flag are retrieved from the RCU table. The nodes that are blocked are not taken into consideration for the following steps. Foremost, the shortest virtual path (V_p) between CI and CB is computed (Fig.4b). The nodes which are at perpendicular position to V_p are taken for route computation (Fig.4b). From these set of nodes, the one with minimum perpendicular distance from V_p and to which CI can transmit without getting exhausted will be the next node (N_2) in the route (Fig.4c). N_2 is considered as the new source (next node for communication) if it has less mobility, minimum perpendicular distance and farthest node from CI but within the proximity of CI. The nodes with less energy are taken as route if that is the only path to reach CB. This is to extend their lifetime. Once the suitable next node (N_2) is found, it is added to RA and the process of route computation between source and CB is repeated until CB is in proximity of the new next node. For the depicted scenario, the route array will be [CI, N_2, N_4, N_6, N_8, N_9, N_{11}, CB]. This procedure gives the shortest path, which has the capacity to facilitate secure transfer of packets without getting the nodes exhausted (Fig.4d). Also, this selection ensures nodes with maximum energy, with least displacement and which are in farthest proximity are participating in communication. Hence nodes with minimum energy do not suffer load due to transmission unless they are the only route to reach the CB. As a result, the PACR provides a better platform in improving the lifetime of a node as well as the network. The algorithm for PACR is given in Table 3.

ISSN: 0975-8585

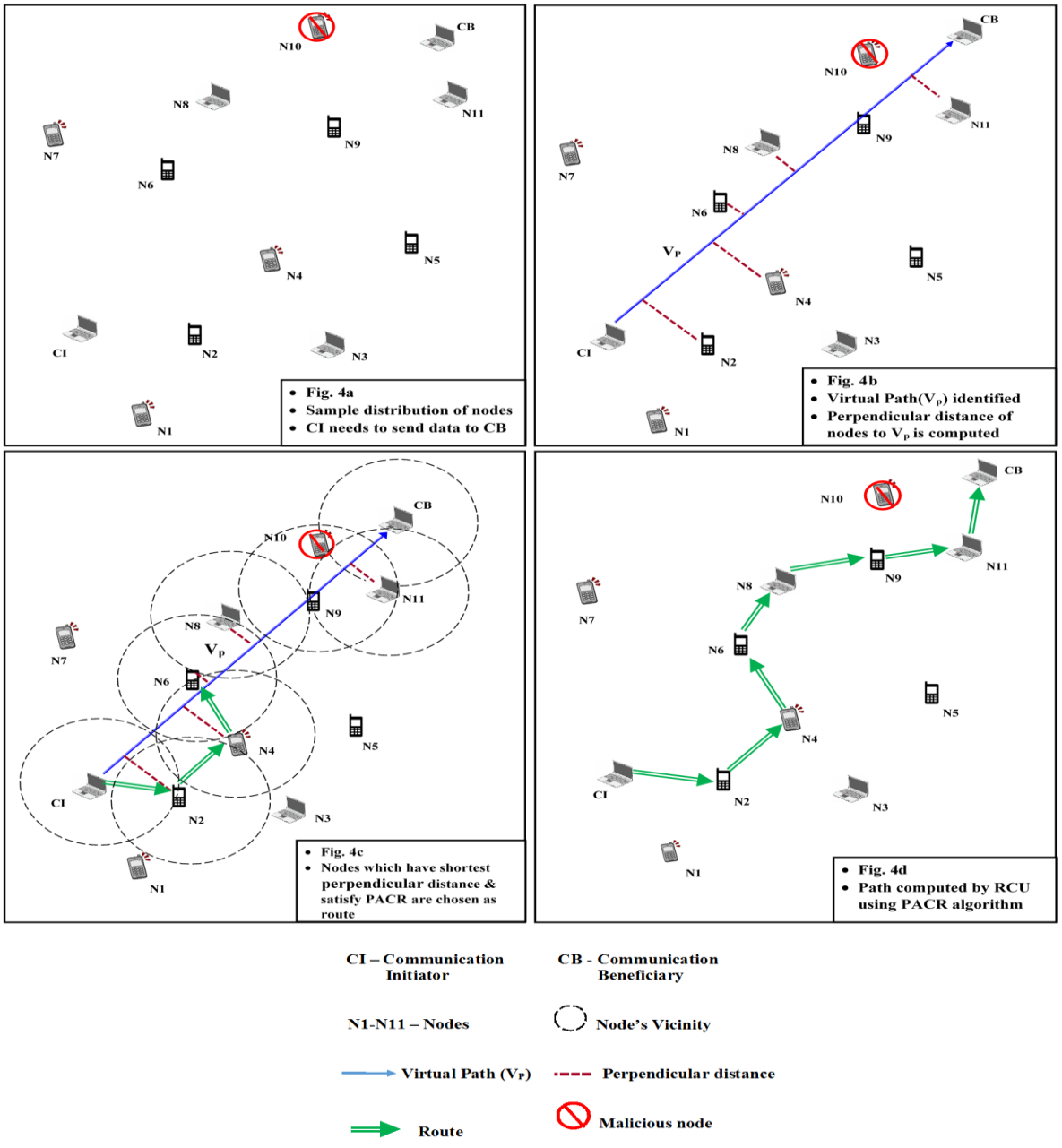

Fig.4 Depiction of Route Computation using PACR.

Table 3 PACR algorithm upon receiving RREQ.

Nomenclature: TA - Temporary array in 2-D form, k- Energy required to transfer one message packet / unit distance, α_1 - Source x-coordinate, β_1 - Source y-coordinate, α_{CB} - Destination x-coordinate, β_{CB} - Destination y-coordinate. Let V_p be of the form $k_1\alpha + k_2\beta + k_3$, where k_1, k_2, k_3 are constants, B_{ft} - Temporary block list and B_f is the block flag of nodes.

Begin

Initialize RA

Set i to1

If(B_f is TRUE for CI || B_f is TRUE for CB)

Discard the RREQ

Else

Set CI-ID to RA[0]

Loop(till RA[i] $\neq$ CB-ID)

If(no node is present within the proximity of source)

Add source to B_{ft}

End if

Calculate Virtual Path V_p to CB,

$$V_p = \frac{\alpha-\alpha_{CB}}{\alpha_{CB}-\alpha_1} = \frac{\beta-\beta_{CB}}{\beta_{CB}-\beta_1}$$

Set j=0

Loop(Through all the nodes under the proximity of the current source node for which $B_f=B_{ft}=0$)

Find the foot of perpendicular, $\frac{\alpha_2-\alpha_1}{k_1} = \frac{\beta_2-\beta_1}{k_2} = \frac{-(k_1\alpha+k_2\beta+k_3)}{k_1^2+k_2^2}$

Calculate distance between (α_1,β_1) and the obtained (α_2,β_2)

Store it in $TA_{[0][j]}$

Calculate distance between RA[i] and (α_1,β_1)

Store it in $TA_{[0][j]}$

End Loop

Set j to 0

Set temp_val to ∞

Loop(through all TA)

$DIST_{PER} = TA_{[0][j]}$

$DIST_{NODE} = TA_{[1][j]}$

Calculate the required transmission energy (E_{MT})

E_{MT} = MSG SIZE x $DIST_{NODE}$ x K

If($DIST_{PER}$ < temp_val)

$E_{diff} = E_n(t) - E_{MT}$

If ($E_{diff} < E_{TH}(n)$)

Set source as the (α_1,β_1)

temp_val = $DIST_{PER}$

End if

End if

End loop

Add source to RA[i++]

End loop

End If

Remove temporary block list elements

End

Processing of Route Array (RA)

The RCU returns a RA to CI which consists of an effective route to CB. The format of the RA is given in Fig.3i. The message size mentioned in Fig. 3j. CI upon receiving the RA from RCU, removes its ID from RA, creates a transmission packet (message packet + RA) and transmits to the first element of RA. When the first node receives the transmission packet (RA and message), it removes its address from RA and transmits the packet to the next element in RA. This process is done until RA is empty. In case the next node to which the message packet to be transmitted is not within the proximity of the previous node, it sends a RREQ to RCU. Once the RCU receives this request it calculates a new route to CB using PACR and returns a new array and communication takes place as per the new RA once again.

SIMULATION AND RESULTS

The proposed methodology is experimented using NetSim standard version simulator. The Table 4 lists the parameters taken for simulation.

Table 4 List of Parameters for Simulation

Parameters	Values
Simulator	NetSim
MAC Layer	IEEE 802.11
Simulation area	1000 meter
Number of nodes	50
Transmission Range for RCU	250 meter
Size of the Cluster	Dynamic
Transmission range for nodes	30 meter
Mobility	Randomized
Simulation time	5400 seconds
Traffic type	CBR
Maximum Transmission rate	20 packets / sec

1: Study of individuals components of a network

The graph (Fig. 5a) shows the variations in energy of nodes within a cluster for a simulation period of 5400 seconds. The graph was observed for a separate cluster (B) in order to emphasize more on the cluster based operations. The operations of the nodes were to manage their internal tasks and also to communicate with their cluster members including update replies to cluster head. The update reply is done to notify the cluster head about the change in their position, present energy, etc., as it is mobile by nature. By the 1800^{th} second a new node (A2) was made to reach the cluster B in order to test its adaptation with the cluster. By the same time multiple message transfers were made from B1 to other nodes which resulted in a steep fall in its energy by 3600^{th} second (Fig. 5a). Throughout the simulation, it is observed that the cluster showed stability due to these tasks and also the lifespan of the network has improved. The Fig. 5b depicts the changes in cluster C and D during the simulation span. At 1800^{th} second, the cluster heads C5 and D2 are within the proximity of each other which made the cluster head election process. This results in D2 as the cluster head. From the Fig. 5c, it can be observed that the cluster D2 showed stability and its energy reduction with time is very minimum though it handled multiple message transactions with many member nodes. The reason for change of cluster head can be seen from the Fig. 5d and the performance is compared with the mobility prediction based protocol (MLR) [20]. The graph shows the energy levels of Node E4 (old cluster head) and E3 (new cluster head) as per PACR algorithm. As the previous cluster head E4 reached the threshold energy (E_{TH}) for being cluster head at 5400th second, the cluster head election is required. This results in E3 as the new cluster head for the cluster E. From the graphs it is evident that our algorithm proved to be better in improving the lifetime of the network than the existing schemes.

ISSN: 0975-8585

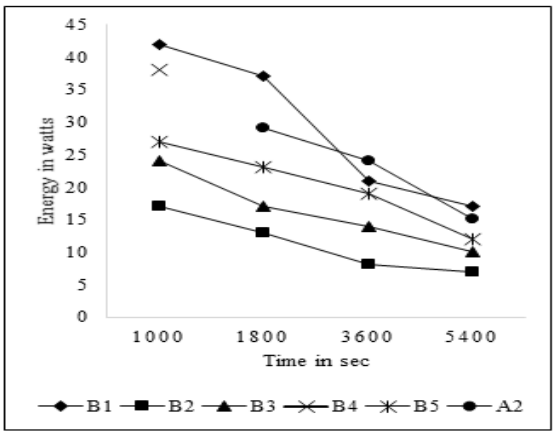

Fig. 5a Energy variations in a Cluster B

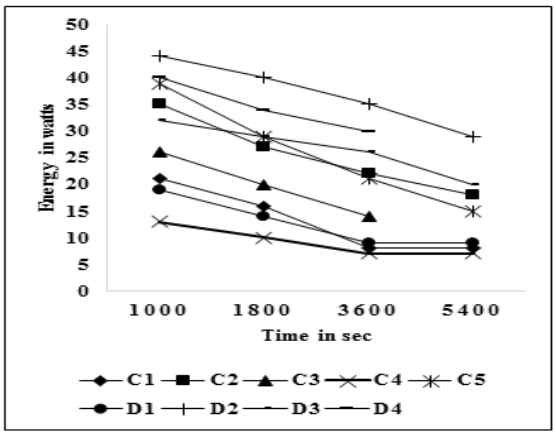

Fig. 5b Energy Variations while Cluster head Election

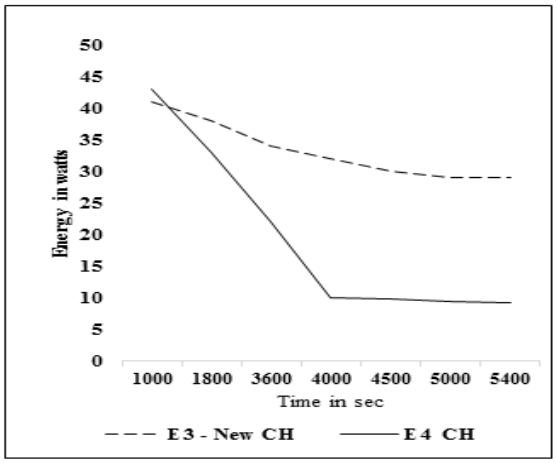

Fig. 5c Change of new cluster head due to E_{TH}

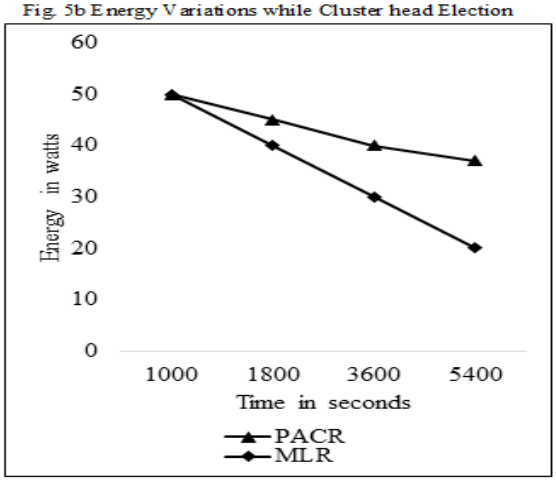

Fig. 5d Comparison of PACR with MLR

Fig.5 Analysis of PACR under various circumstances

Study 2: Study of the network on the whole

Apart from the study of individual components, the entire network (Fig.6) is comprehended from the simulation. The entire network performance is studied for the period of 5400 seconds. The energy levels of nodes under various circumstances are monitored and ensured that a node with very low energy sustains in the network for longer period of time because of the PACR algorithm.

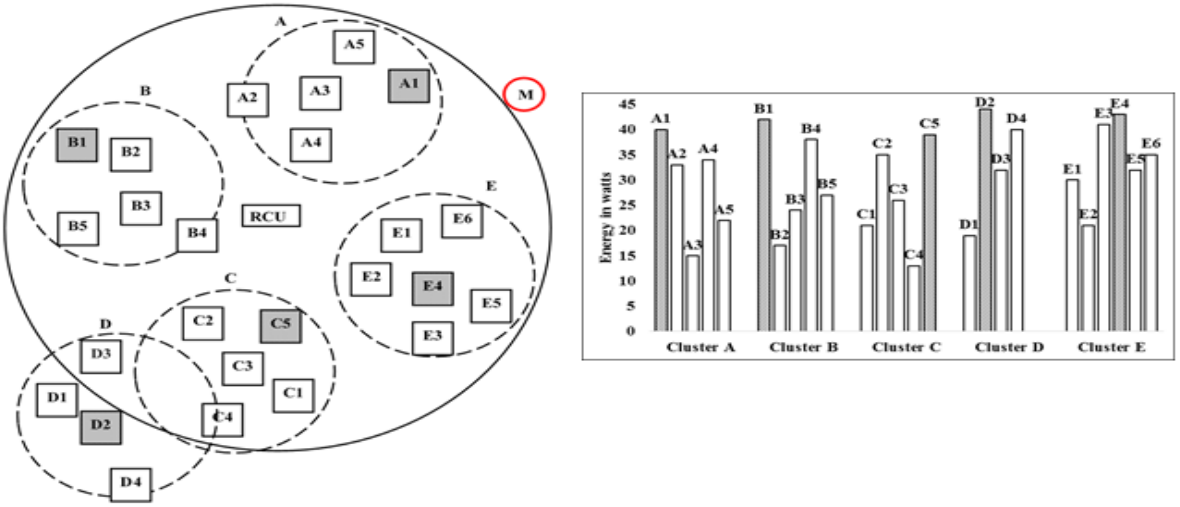

Fig. 6 Initial Position of Nodes and their Energy Levels

ISSN: 0975-8585

Simulation scenario

The network consists of a total of 49(+1 malicious node) nodes divided into 5 clusters (A to E). For the depiction clarity, only 25 actively participated nodes are shown in the Fig. 6. The cluster head election was made to occur simultaneously for the respective clusters. Also to check the defensive capacity of the network, a malicious node was made to move towards the network. The node A2 of cluster A is at the edge of its cluster and moves away from cluster A and node B4 from leaves the cluster B. The clusters C and D are moving towards each other. The energy level of nodes at this time is depicted by the graph in Fig. 6.

At 1800th second, the malicious node M has entered the network into cluster A (Fig. 7). The A1 performs the security check on the new node M and declares it to be malicious and sends a malicious node alert to its members. Although the malicious node is within cluster A, the node is not taken into consideration as it has to be ignored. The node B4 forms its own cluster as it is not under the vicinity of any other cluster which is depicted in the graph of Fig. 7. The node A2 that left the cluster A, entered into cluster B and adopted by the cluster head B1 after the security check. The energy levels at this duration is depicted in the graph of Fig. 7.

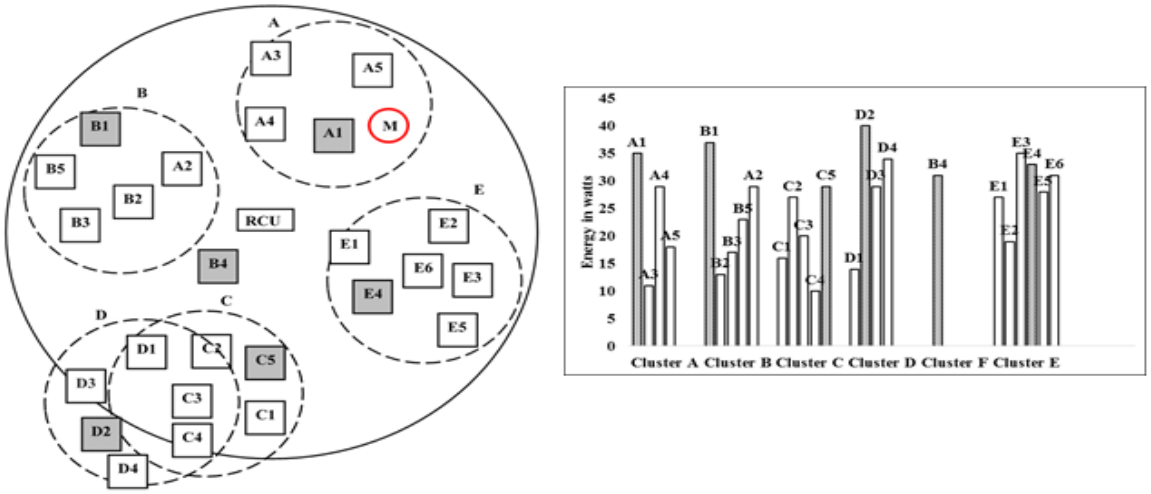

Fig. 7 Position of Nodes and their Energy Levels at 1800th second

During 3600th second (Fig. 8) it is evident that there is a change in members of clusters C and D. Two cluster heads C5 and D2 arrived within the proximity of each other which caused the cluster head election (Refer 3.2.2). Now the members of cluster C and the cluster head C5 become the members of cluster D. This increases the number of clusters in D. This is because of greater capacity of the D2 of cluster D to function as a cluster head. The energy levels of all the nodes and their cluster heads are shown in the graph of Fig. 8.

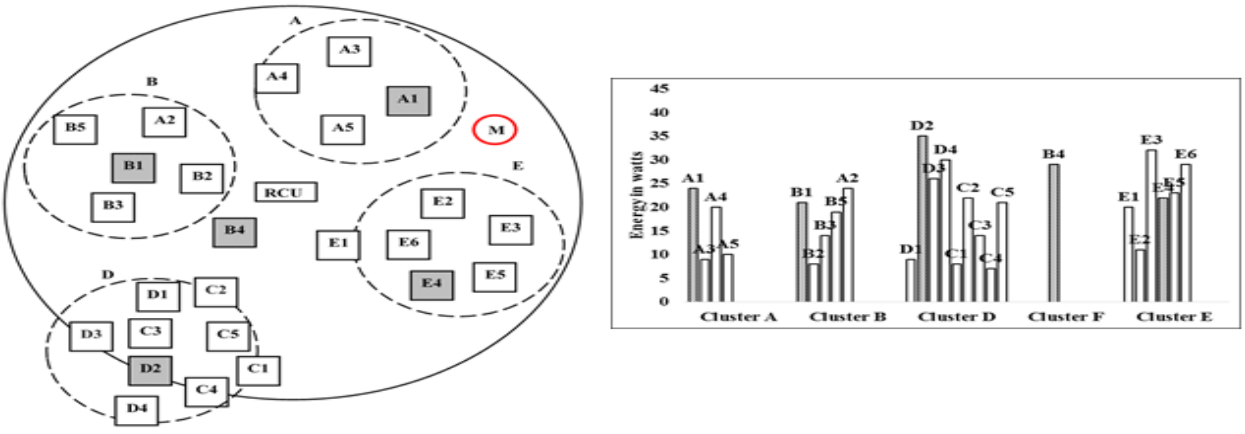

Fig. 8 Position of Nodes and their Energy Levels at 3600th second

ISSN: 0975-8585

At the end of simulation span (5400th second) the nodes D1 and C4 left the network and lose their cluster member identity (Fig. 9). The node B4 that left B and formed its own cluster is having a node E1 as its member. Also a series of inter and intra cluster communications were made to happen between the nodes of cluster F and E. The multiple message transmission between nodes in cluster E results in a heavy drop in energy of E4 (Fig. 9), which reached the threshold value $E_{TH.}$ Hence cluster head election takes place; the node E3 has been chosen as new cluster head for the cluster E. It is observed from the Fig [6-9] the nodes which are having less energy is not being used for communication unless they are the only route to the destination node. Hence the energy of such nodes are retained their lifetime is improved. When a cluster head loses its energy and reaches the threshold energy, then cluster head election occurs to preserve the energy of the cluster head to function as a normal node within the network.

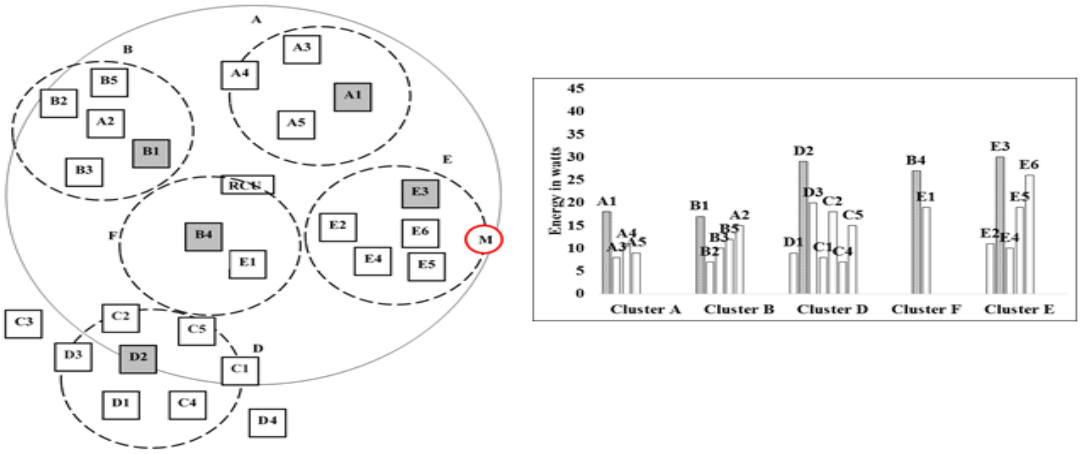

Fig. 9 Position of Nodes and their Energy Levels at 5400th second.

From the simulations, it is observed that, even though constant monitoring and update cycles are done by cluster heads, the energy drain is very minimum. The nodes taken into consideration were weak nodes with high energy drain per task, yet the nodes sustained for a longer period of time. As a result, authenticated nodes with various capabilities and functions can actively participate in network activities for longer period of time as far as load balancing is done. The above results prove PACR to be efficient than other routing techniques. The increase in threshold energy of cluster head represents the fact that when the node reaches this value it can easily be functioning as a normal node after electing the new cluster head.

CONCLUSION

In this paper we proposed Position Aided Cluster based Routing (PACR) to effectively balance the transactions through the nodes in a network. This provides a secure network, free from malicious node attacks, thereby preventing the loss of packets. We modified the traditional paradigm for a MANET by adding a Route Computation Unit which used the PACR algorithm, dynamically providing nodes with a perfect load balanced route for safer transmission of packets swiftly. It proves itself better than all available load balancing techniques by improving the network lifetime significantly. In the situation of link failure, upon request, with no further delay, the RCU supports the nodes for rerouting This approach was supported by the simulated results and thus we obtain the following merits: improvement in robustness of topology by supporting the network, provision for link rebuilding thereby leading to a very secure and stable network, reduced overhead time, increased lifetime of the network and reduced delay by utilizing the effective nodes. The entire network was observed to be very stable, secure and had improved lifetime.

REFERENCES

[1] [1] C. E. Perkins and P. Bhagwat, Highway Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers 1994; In proceeding of the ACM SIGCOMM '94 ; 234-244.

[2] [2] Sung-Ju Lee, Elizabeth M. Belding-Royer and Charles E. Perkin. Scalability study of the ad hoc on-demand distance vector routing protocol. International Journal of Network Management 2003; 13:

97–114. DOI: 10.1002/nem.463

[3] [3] Shin-Jer Yang. Design issues and performance analysis for DSR routing with reclaim-based caching in MANETs. International Journal of Network Management 2010; 20: 21–34. DOI: 10.1002/nem.726

[4] [4] Kaur, S., Kaur, S., and Mohali, M. Analysis of zone routing protocol in MANET. International Journal of Research in Engineering and Technology 2013; 02: 520–524.

[5] [5] Guo, Z., Malakooti, S., Sheikh, S., Al-Najjar, C., & Malakooti, B. Multi-objective OLSR for proactive routing in MANET with delay, energy, and link lifetime predictions. Applied Mathematical Modelling 2011; 35(3): 1413–1426. DOI:10.1016/j.apm.2010.09.019

[6] [6] Marina, M. K., and Das, S. R. Ad hoc on-demand multipath distance vector routing. Wireless Communications and Mobile Computing 2006; 6:969–988. DOI: 10.1002/wcm.432

[7] [7] Saigal, V., Nayak, A. K., Pradhan, S. K., & Mall, R. Load balanced routing in mobile ad hoc networks. Computer Communications 2004; 27(3): 295–305. DOI:10.1016/j.comcom.2003.09.002

[8] [8] Islam, M., Razzaque, A., Bosunia, M. R., Alamri, A., & Hassan, M. M. Link failure and congestion-aware reliable data delivery mechanism for mobile ad hoc networks. Annals of Telecommunications 2012; 68(9-10): 539–551. DOI: 10.1007/s12243-012-0339-2

[9] [9] Conceição, L., & Curado, M. Onto scalable wireless ad hoc networks: Adaptive and location-aware clustering.Ad Hoc Networks 2013; 11(8): 2484–2499: DOI: http://dx.doi.org/10.1016/j.adhoc.2013.07.001

[10] [10] Gayathri Venkataraman, Sabu Emmanuel and Srikanthan Thambipillai. Size-restricted cluster formation and cluster maintenance technique for mobile ad hoc networks. International Journal of Network Management 2007; 17: 171–194. DOI: 10.1002/nem.643

[11] [11] Fouda, M. M., Nishiyama, H., Miura, R., & Kato, N. On Efficient Traffic Distribution for Disaster Area Communication Using Wireless Mesh Networks. Wireless Personal Communications 2013; 74(4): 1311–1327. DOI: 10.1007/s11277-013-1579-9

[12] [12] Georgios Kioumourtzis, Christos Bouras and Apostolos Gkamas. Performance evaluation of ad hoc routing protocols for military communications. International Journal of Network Management 2012; 22: 216–234. DOI: 14 September 2011

[13] [13] Tashtoush, Y., Darwish, O., & Hayajneh, M. Fibonacci sequence based multipath load balancing approach for mobile ad hoc networks. Ad Hoc Networks 2014; 16: 237–246. DOI: http://dx.doi.org/10.1016/j.adhoc.2013.12.015

[14] [14] Tomar, G. S., Shrivastava, L., & Bhadauria, S. S. Load Balanced Congestion Adaptive Routing for Randomly Distributed Mobile Adhoc Networks. Wireless Personal Communications 2014; 77:2723–2733. DOI: 10.1007/s11277-014-1663-9

[15] [15] N.C. Wang. Power-aware dual-tree-based multicast routing protocol for mobile ad hoc networks. The Institution of Engineering and Technology 2012; 6: 724–732:. DOI: 10.1049/iet-com.2011.0073

[16] [16] Paramartha dutta a , Anuradha Banerjee. Fuzzy-controlled Power-aware Multicast Routing (FPMR) For Mobile Ad Hoc Networks. Procedia Technology 2012; 4: 38-49. doi: 10.1016/j.protcy.2012.05.005

[17] [17] Budyal, V. R., & Manvi, S. S. ANFIS and agent based bandwidth and delay aware anycast routing in mobile ad hoc networks. Journal of Network and Computer Applications 2014; 39: 140–151. DOI: 10.1016/j.jnca.2013.06.003

[18] [18] Bin Yang, Jinwu Xu, Jianhong Yang and Debin Yang. A novel weighted clustering algorithm in mobile ad hoc networks using discrete particle swarm optimization (DPSOWCA). International Journal of Network Management 2010; 20: 71–84. DOI: 10.1002/nem.73

[19] [19] Kui Wu and Janelle Harms. Multipath Routing for Mobile Ad Hoc Networks. Journal of Communications And Networks 2002; 4: 48-58.

[20] [20] William Su, Sung-Ju Lee, and Mario Gerla. Mobility prediction and routing in ad hoc wireless networks. International Journal of Network Management 2001; 11:3–30.