ISSN:0975-9646
R S Shaji et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (5) , 2010, 355-362

An Efficient Routing scheme for reliable path establishment among Mobile Devices in Heterogeneous Networks

R S Shaji[1], R S Rajesh[2], B. Ramakrishnan[3]

[1]*Department of Computer Applications, St.Xavier's Catholic College of Engineering, Kanyakumari, India*
[2]*Department of Computer Science, ST. Hindu College,, Kanyakumari, India*

[3]*Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India*

***Abstract*- In heterogeneous networks, devices available with varying connectivity help to provide many new opportunities for efficiently utilizing new resources. In mobile ad hoc networks with varying layered architecture, not much interest is given yet in establishing path among devices with increasing or decreasing in number of mobile devices in the network and the complexity in using them because of their mobility. In this paper, we have considered the various aspects of routing in order to find out the proper nodes in the network and establish a reliable link in a heterogeneous environment. A new Routing scheme called SFUSP (Self-eliminating Fault-tolerant based Un-interrupted reliable Service switching mobile Protocol) is discussed which is specially designed for establishing path among devices in heterogeneous environment in pervasive spaces. Our routing scheme is based on proactive routing characteristics with further added dynamism in selecting better nodes in the routing path in the heterogeneous networks. Performance analysis of our routing scheme is compared to other existing manet protocols such as AODV, DSR and OLSR in Random Waypoint, Brownian and Manhattan mobility models under MAC layers IEEE 802.11, 802.15 and 802.16 for WIFI, WPAN and WIMAX networks. Our routing scheme shows better performance for the above mentioned standards and is well suited for pervasive environment.**

***Keywords*- Manet, Self-elimination, WIFI, WPAN, WIMAX, MAC, pervasive.**

I. INTRODUCTION

A Mobile Ad-hoc Network (Manet) is composed of Mobile Nodes without any infrastructure. Mobile Nodes self-organize to form a network over radio links. In this environment, multicast routing protocols are faced with the challenge of producing multi-hop routing under host mobility and bandwidth constraints [01]. Wireless service providers have started offering numerous data services over their networks through various types of channels and for different types of accessing devices. With all these diverse technologies coming together, requirement of anywhere, anytime data access on any device had been provoked, which has taken shape to ubiquitous Computing [02]. A framework for wireless mobile pervasive computing is considered to augment capabilities and to save scanty resources of mobile host by making full use of available resources in the surrounding [03].

Clustering of devices in MANET could reduce overhead, flooding and collision in communication and make the network topology more stable. Cluster Heads are determined dynamically and are in charge of the routing of the cluster. The Location Aided Hierarchical Cluster Routing is a more suitable way for mobile adhoc network routing [04]. The challenges in wireless, mobile inter-domain routing include dynamic network topology, intermittent connectivity, and routing protocol heterogeneity [05]. But they are not clearly addressed in these papers for high mobility nodes with varying mac layers.

The performance of routing protocols in Mobile Ad hoc network is always dependent on the availability and stability of wireless links [06]. Topology control in mobile ad hoc networks (MANET) is needed for reducing interference collisions and in consequently retransmission [07]. Various multicast routing protocols with distinguishing feature have been newly proposed and discussed in [08]. Location-based routing is difficult when there are gaps in the network topology and nodes are mobile or frequently disconnected [09]. Also, it is necessary to control the broadcasting mechanism to avoid flooding of control messages and one mechanism is discussed in [10]. An efficient Path discovery is needed and an integrating mechanism for path discovery in Manets on the proactive OLSR protocol is discussed in [17]. Performances such as higher packet delivery ratio, lower average end-to-end delay and lower normalized routing overhead are needed for any routing path discovery protocols. A comparative study on the routing performance of two reactive routing protocols for mobile Ad hoc networks is discussed in [18]. But proactive protocols are performing better than reactive protocols for static networks and are not good for dynamic networks. But, our proposed scheme is developed with added dynamism in proactive characteristics of a routing protocol [20] such as clustering and self-elimination, that helps in improving the performance for higher mobile devices with better communication and resource strength under heterogeneous environment.

The mobility model is one of the main aspects for testing the performance of MANETs routing protocols [11]. The performance of routing protocols in a Mobile Ad hoc Network is related to the network topology and nodes mobility [12]. Mobility models also affect the performance of ad hoc routing protocols and can be divided into entity mobility and group mobility models [13]. In most real environments, however, very commonly a group or multiple groups move under the direction of a group leader or group leaders rather as independent individuals [14]. We have compared our scheme in various mobility models such as Random Waypoint, Brownian and Manhattan model.

There are difficulties in developing an information dissemination mechanism for heterogeneous environments and the problem may be encountered in handling different medium of access control layers. The problems encountered when designing a solution for IEEE 802.11 ad hoc networks and for high and low traffic scenarios, with nodes in close proximity is discussed in [15]. Mobile Wimax is a fast growing broadband access technology that enables low-cost mobile Wimax with flexible bandwidth and fast link adaptation is discussed in [16]. The IEEE 802.15 standard has received considerable attention in academy and industry as a low data rate and low power protocol for WSNs is discussed in [21].

SFUSP is an efficient path discovery scheme which maintains information regarding route status, speed of nodes, medium of access of devices and clustering details of the network. It works on the basis of proactive characteristics of a routing scheme. In addition, it elects node form the cluster by comparing the node strength on the basis of their communication speed, resource strength and mobility and is done by the nodes themselves.

II. RELATED WORKS

The routing performance is greatly dependent on the availability and stability of wireless links. Although there are some studies reported to evaluate the performance of routing protocols in MANET, little work is done for the overall performance of the system [06]. Topology control in mobile ad hoc networks (MANET) tries to lower searching methods by reducing collisions and consequently lowering retransmission is discussed in [07]. Various multicast routing protocols with distinguishing features have been newly proposed and a survey of the multicast routing protocols is discussed for various metrics is discussed in [08]. Location-based routing is difficult when there are gaps in the network topology and nodes are mobile or frequently disconnected is discussed in [09]. AODV protocol analyses the lifetime of node when implementing routing discovery and avoiding the unnecessary information are being sent efficiently is discussed in [10]. But, all above protocols are not well suited for path establishment among the nodes with varying mobility, with varying mac layers under varying user interfaces in heterogeneous networks. Our scheme eliminates the drawbacks mentioned above in maintain a good performance under the above stated environment.

III. SFUSP – A RELIABLE ROUTING SCHEME

A. Self-eliminating Fault-tolerant based Un-interrupted reliable Service switch mobile Protocol (SFUSP)

Self-eliminating Fault-tolerant based Uninterrupted reliable Service switching mobile Protocol (SFUSP), is a protocol specially designed for pervasive computing environment for Manets. It is basically a proactive protocol with additional functionality added such as clustering and self-elimination. It is a well supported context-aware and fault-tolerant service discovery routing protocol. SFUSP is reliable while searching the exact service offering node and thus, it reduces the searching time and balance load among the nodes which are all involved in the process of discovery in heterogeneous networks.

SFUSP follows a new technique to eliminate less strengthened nodes (ie. Low Resource, Low Power, Low Bandwidth and Unstable) which get connected during the path discovery process. The additional task of refreshing the existing list of nodes will be reduced, if the unwanted nodes get eliminated in the time of path discovery itself. SFUSP will keep only the best selected node details in its database.
SFUSP is as intelligent as a reliable manet routing scheme for any heterogeneous environment which can along with any service discovery protocol, can help in providing good service provisioning.. Location based systems can be used along with this scheme for the unfavorable situations to find the previous servicing location details and a new link can be established, if the service gets interrupted due to non-availability of nodes nearby the link.

The routing scheme contains three main functionalities such as clustering, self-elimination and routing path establishment and the diagrammatic representation is in Fig: 1. The steps involved under SFUSP routing scheme are as follows,

Step01: Broadcast the message to discover the node which is requested by the requester node.
Step02: If Unfound then representative nodes will be activated to generate a new search in their nearby locations.
Step03: If requester node is found then
Step04: Group all the representatives by location.
Step05: Find the most reliable representative.
Step06: Do the self-elimination technique to reduce to best suited nodes in order to find the most reliable path.

Step07: Establish the reliable path with the best strengthened nodes in the path.

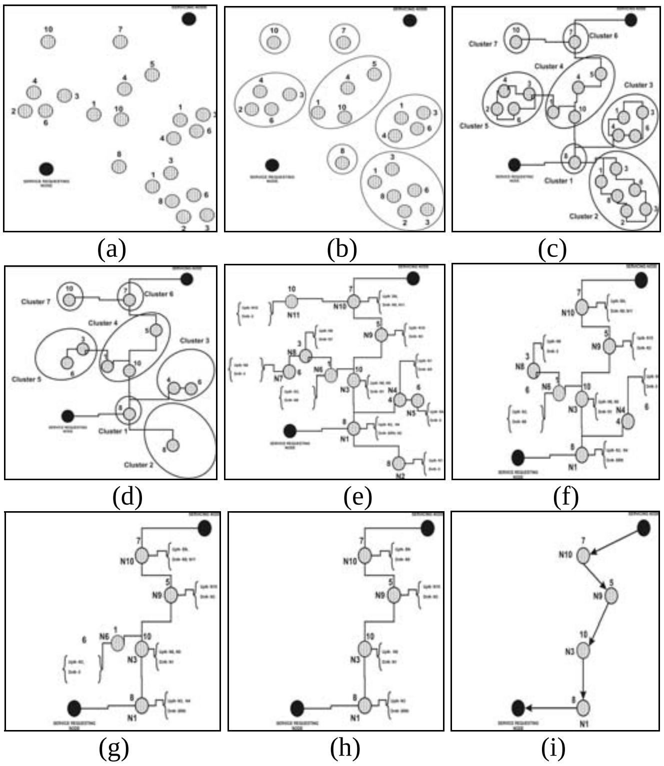


Fig: 1 (a) SFUSP node Discovery (initial stage), (b) SFUSP nodes Clustering, (c) SFUSP Cluster Linking, (d) SFUSP Elimination Session starts, (e,f,g,h) SFUSP Elimination Sessions, (i) SFUSP finds a Reliable Service Path.

The Nodes with black shade represents the service requester and service provider for a time instant. Other nodes may be representative nodes in the route path or nodes in the network. Next we will see how all the nodes in the network are made under a cluster by using the clustering algorithm in Fig: 2.

A1. Clustering

After the eligible nodes are selected, they are grouped by locations by using a clustering algorithm as shown in fig: 1, where no node will be excluded from any of the available clusters. Grouping of nodes in the cluster under an area is done through a location based system. If the area increases, number of clusters also increases.

Algorithm : Clustering

Algorithm CLUSTERING ()
Ci← 1(Initialize);
Node[i]←list of nodes in the area
Area[i] ← Area ID //Get the area list
For each Area[i] do
    For each node[i] do
        NodeClusterID ← Ci
    NodeAreaID ← Area i
    End For
Ci←Ci+1
//when area increases the no. of cluster also get increases
End For
End

Fig: 2 Algorithm for Clustering

In the clustering process, IP geo-location based metrics [23] is used for the localization of nodes by considering the scalability of the network. Distance approximation is done on the basis of transmission capacity of a node and the communication area occupied by the network.

Clustering enables the comparison of better strengthened node in that area. In manets, nodes often change their native cluster due to the mobility and so get reduced in the efficiency of communication among source and destination. The comparison among the nodes may be done among themselves by using a technique called self-elimination and the procedure is given in fig: 3.

Now the time taken for individual node and all clusters are calculated by their data length, transmission rate and their delay values. Time taken for single node simulation for any nodes in the network can be calculated as follows,

$$\left(\frac{DataLength}{TransmissionRate}\right) X\ TransmissionDelay \quad \ldots. \quad (1)$$

Cluster simulation time can be calculated as the total number of clusters available in the network with the data length to the transmission rate of each node in the cluster multiplied with the transmission rate. It is calculated as follows,

$$\left(\frac{Total\,Number of\,Nodes\ \text{in}\ acluster\ X\ DataLength}{\sum_{i=0}^{n} TransmissionRate_i}\right) X\ TransmissionDelay \quad \ldots.. \quad (2)$$

A2. Self-elimination Process

The highlight of the SFUSP routing scheme is the self-elimination procedure that helps in finding the most strengthened node in the cluster. Along with the proactive nature of the scheme, the self-elimination process finds effective node in the cluster for establishing reliable links on the basis of the strength of the nodes. The strength may be calculated with the context specified by the requester and the packet structure is given in the next section. The following algorithm in Fig: 3 illustrate the processes involved in the self-elimination technique.

Algorithm : Self-elimination

```
Algorithm SELF_ELIMINATION()
cluster_nodes[i] ← all node ids in the cluster
me_node_id ← service providing node id
Threshold ← n
DownNode(x) ← Service request node ids
Up_Node← original first service request node id
for each cluster_nodes do
        if (cluster_nodes[x].DownNode(x) ≠ "empty")
        {
                If(cluster_nodes[x].strength ≥ threshold)
                {
                        cluster_nodes[x]← "alive"
                        //context service found
                If (cluster_nodes[x].context =
                                me_node_id.context) then
                // check the context
                {
                If (service request node ≠ null)
                {
                        Send message to service request
                        node    (Up Node) "chosen"
                }
                End if
                If (Up_Node ≠ null) then
                //to check the node reached the original
                                first location
                {
                Send message to Up_node "Path Fixed"
                }
        End if
        }
        Else
        //if context not matched and threshold value is not
        satisfied
        {
                cluster_nodes[x] ← Representative node
        }
        End if
        }
        else


        //if the node has no strength means it can be in a
          not alive stage
        {
                cluster_nodes[x] ← "not alive"
        }
        End if
        }
        else
        {
                cluster_nodes[x]← "not alive"
        }
        End if
        //if the path is fixed and the node is not selected
        means   it can be not alive by it-self
        If (cluster_nodes[x].message = "path fixed") then
        {
                If (cluster_nodes[x] ≠ "chosen") then
                        {
                        cluster_nodes[x] ← "not alive"
                }
                End if
        }
        End if
End if
End For
End
```

Fig: 3 Algorithm for Self-elimination.

In the self-elimination process, each node will collect the information about their service providing and service requesting nodes ie. Up and down nodes. Then, the nodes which have not participated in the routing process in the list will be deleted first and this will be repeated until a reliable path is established. In fig: 1(a), the requested nodes are discovered during the path establishment process. The two black shaded nodes in the figure represent the source and destination nodes. The intermediate nodes are the nearby nodes or nodes in the coverage area. In fig: 1(b), all the nodes are clustered on the location basis. Each node is represented by a value which indicates the strength of the node on the basis of bandwidth, connectivity etc. All the location wise identified clusters are linked together and so, a location may contain n-clusters. From which the best suited node in the cluster will be selected by the self-elimination process.

In the first session of elimination, all the grouped clusters, unwanted or low strength nodes will be eliminated. In each group, a comparison will be done to find the most strengthened node to establish a reliable path. Fig: 1 (c) and (d) illustrates the cluster linking and the start of elimination session. In the elimination session, in Fig: 5, all the weak and unreliable nodes are get eliminated from the reliable link. By this, we can get an exact and reliable path to continue with the communication.

This is an intelligent elimination technique, where most reliable path can be set by removing the less reliable nodes which still get connected after the session of elimination. Here each node has to generate a list of Upper Node (UpN) and Down Node (DnN) detail from their connection establishment. After generating this list, the nodes which have no Down Node (DnN) can be voluntarily got off from the connection establishment. Both the elimination and clustering processes are done without the knowledge of the service requesting node.

Finally, the most reliable path for routing in the network will be established as in the Fig: 1(i) . The communication will be done through this path. The path will get often changed in the mobile environment and so the process is repeated at once with any node that senses the nearby node that is left or a new node that gets entered in the cluster or un-necessary nodes in the link.

Simulation time of non-eliminated nodes in a cluster can be calculated as the total number of current nodes present in the cluster with the sum of the node data length to the sum of the transmission rate of all nodes multiplied with transmission delay. The non-eliminated nodes in the cluster can be calculated as follows,

$$\left(\frac{Total\,Number of\,Current\,Nodes\,presnet\,in\,a\,Cluster\;X \sum_{i=0}^{n} Node_i\,DataLength}{\sum_{i=0}^{n} TransmissionRate_i} \right) X\,TranmissionDelay \quad \ldots\ldots \quad (3)$$

Now, we can calculate the self-elimination time of a node in the cluster by the following formula,

$$Cluster\,SimulationTime - Non - Eliminated\,Nodes\,SimulationTime\,of\,a\,Cluster \quad \ldots. \quad (4)$$

The routing process taking place during the path discovery is illustrated in the following algorithm in Fig: 4.

A3. Routing

The routing process comprises of the clustering followed by the self-elimination technique in each cluster.

Algorithm : Routing

Algorithm ROUTING_PROTOCOL_SFUSP(list

_of_replied_nodes)
Location_Li ← All Geographic Location List of the replied

nodes
call CLUSTERING();
If (service='established') then
for each Location_L_i Do
$Node_i$ ← All Nodes in the Location L_i
for each Node in L_i Do
If $Node_i$ greater in the group then
Keep the Node Alive
call SELF_ELIMINATION()
else
Delete the node from the Cluster;
End If
End For
End For
End If
End

Fig: 4 Algorithm for Routing.

Our aim is to find a better path establishment time with minimum number of effective nodes in the service path which is established in a less number of time. The path Establishment time can be the sum of the cluster simulation time and is given as

$$\sum_{i=0}^{n} Cluster_i\,SimulationTime \quad \ldots\ldots \quad (5)$$

Our performance analysis in the next section clearly shows the efficiency of the proposed routing scheme with respect to other protocols. Because of the effective clustering process and self-elimination technique we have discussed earlier, our routing scheme shows better performance in packet delivery ratio, average end-to-end delay, normalized routing overhead and path establishment time.

IV. PERFORMANCE ANALYSIS

A. Packet Structure

The packet structure for broadcasting, service requesting and service providing is given below. The broadcasting packet structure contains the broadcasting node address, packet type, context which contains individual node characteristics with user interface of requester, location status and is represented by

<Service-Requester-Address, Packet_type, Context, Location_id, Mac_id, user_interface_type >.

For service requesting packet contains the service requester address, the packet type, context searched with the user interface, state of the requester, distance status, cluster status, transfer rate, radio range and delay details and is given as

<Service-requester-address, Packet_type, Context, Location_id, Mac_id, user_interface_type, Transfer_rate, Radio_range, Radio_delay>.

The service provider uses the packet structure which contains service requester as well as service provider address, the packet type, its service description with user interface, state of the node, location, transfer rate, radio range and delay. The packet structure is given as

<Service-provider-Address, Service-requester-address, Packet_type, Context, Location_id, Mac_id, user_interface_type, Transfer_rate, Radio_range, Radio_delay>.

B. Simulation Environment

The simulation is done in network simulator ns2.34 [19], which is a discrete event simulator. The above mentioned packet structures are used for broadcasting, requesting and providing the data for communication. Various networks such as IEEE802.11, 802.15 and 802.16 are tested under their corresponding mac layer. For about 10 services as contexts are assigned randomly to all nodes with varying node density of 50, 100, 200 and 400. The pervasive discovery protocol (PDP) [22] implemented in Ns2 is used for service provisioning in the environment. The mobility scenario is set to Random Waypoint, Brownian and Manhattan Model. The testing was compared with other manet reactive protocols like AODV, DSR and proactive protocol OLSR.

C. Parameters

The parameter is set to the following values and the testing was done under normal conditions.

Network Area	1500 x 1500 m
Channel Type	Wireless
Propagation Model	Two Way Ground
Radio Range	100 m
Radio Delay	10 ms
Traffic Type	CBR
Duration	200 Seconds
MAC Layer	IEEE 802.11, 802.15 & 802.16
Protocol	SFUSP, AODV, DSR, OLSR
Mobility	Random Waypoint, Brownian, Manhattan Model.
Node Strength	Energy, Bandwidth, Context, Node Speed
Context	Contexts such as internet, disk, printer, games etc.. are arbitrarily assigned to all nodes.
No. of Nodes	50, 100, 200, 400
Speed	25 m/s with a pause time of 10 ms. Manhattan min. speed 25 m/s and max. speed 100 m/s.
Transmission rate	9.6 Kbps
Data Payload	512 bytes
Traffic Load	Packet Sent in Every 10 ms

Fig: 5 Simulation Parameter Values

D. Metrics

D1. Packet Delivery Ratio

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source) [11][14]. It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol.

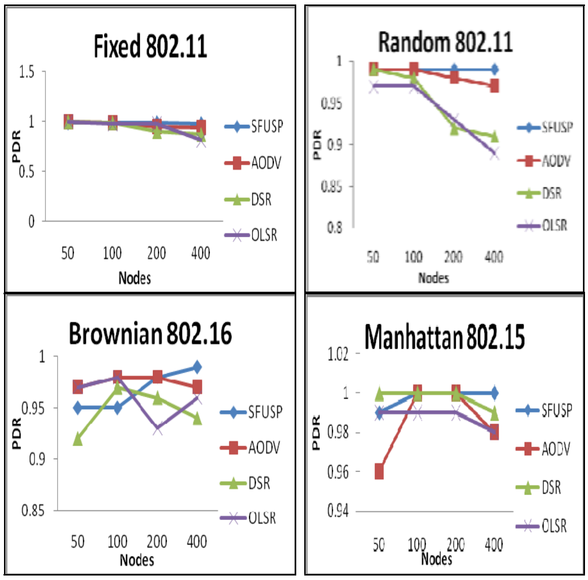
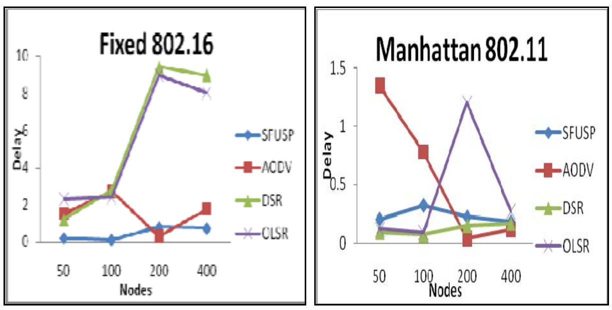


Fig: 6 Packet Delivery Fraction of various protocols under Fixed, Random, Brownian and Manhattan Mobility Models with mac layers IEEE 802.11, 802.15 and 802.16

For Fixed network under the mac layer 802.11, all the protocols are performing in constant with lesser number of nodes and SFUSP shows a constant performance with the increasing number of nodes. This is because of the proactive nature of the protocol where the node status is known in advance. For random mobility in 802.11 mac layer, SFUSP shows a consistent efficiency because of the nature of the mac and the mobility. For Brownian motion with 802.16 mac layer, our protocol shows a progress in performance because of the clustering and self-elimination is limited to a specific area. For Manhattan model in 802.15 mac layer, once again our protocol scheme shows a good performance because of the mobility nature of the node in the model which is well cooperated with the clustering and self-elimination technique.

D2. Average End-to-End Delay

The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination [06][11].



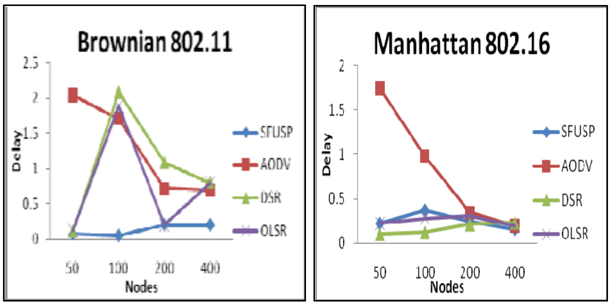


Fig: 7 Average End-to-end Delay of various protocols under Fixed, Brownian and Manhattan Mobility Models with mac layers IEEE 802.11 and 802.16

Average end-to-end delay for Fixed network in 802.16 mac shows, our protocol scheme is consistent because of the constant packet delivery ratio. For Manhattan model under 802.11 mac, our scheme shows better performance when the number of nodes increases. This is because of the combined nature of the proactive character of node movement and dynamism in clustering through which a predetermined path can be established. For Brownian motion under mac 802.11, our scheme shows a consistent performance because of the cooperation of the underlying nature of the mac in Brownian type mobility and the self-elimination process. For Manhattan model with 802.16, because of the predetermined path of the model and the speed of the node, our scheme performs well.

D3. Normalized Routing Overhead

The number of routing packets is transmitted for every data packet sent. Each hop of the routing packet is treated as a packet. Normalized routing load are used as the ratio of routing packets to the data packets [11]. For Fixed network with mac 802.11, SFUSP shows a constant performance because of the proactive nature and the speed in which it forms the path. For Random mobility with 802.16 mac, because of the limited transmission capacity of the underlying mac, our scheme captures the best

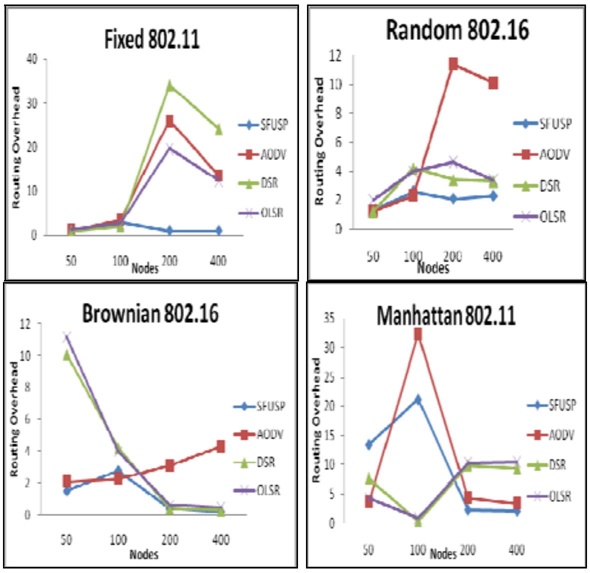


Fig: 8 Normalized Routing Overhead of various protocols under Fixed, Random, Brownian and Manhattan Mobility Models with mac layers IEEE 802.11 and 802.16

nodes as early as possible and so reduces the routing overhead. For Brownian motion with mac 802.16, our scheme shows a constant performance because of the nature of the predetermined motion of the nodes with increasing in nodes. For Manhattan model under 802.11 mac, SFUSP performs well for increasing number of nodes because of the number of clusters it creates and of the proactive nature in maintaining the path.

D4. Routing Path Establishment Time

Path establishment time is calculated from the time taken for simulating all clusters available in the network by the self-elimination process.

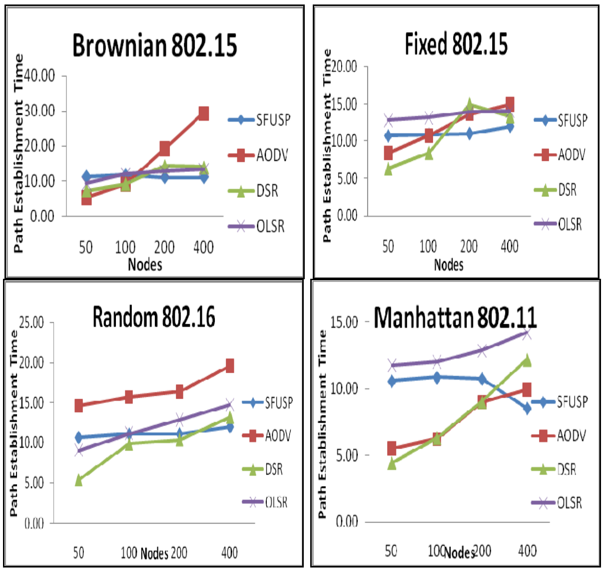


Fig: 9 Normalized Routing Overhead of various protocols under Fixed, Random, Brownian and Manhattan Mobility Models with mac layers IEEE 802.11, 802.15 and 802.16

For Brownian motion under mac 802.15, SFUSP shows a constant performance although the number of nodes is increased and is because of the movement of the node and the area of transmission capacity of the underlying mac layer. For Fixed network under mac 802.15, SFUSP is showing a constant performance than other protocols because of the predetermined topology of the network. For Random mobility under 802.16 mac, our scheme performs better because of the transmission limit of the network. For Manhattan model under 802.11 mac, our scheme takes less time than other protocols because of the predetermined path and the mobility speed of each node. Performance is good for increase in number of nodes because of the combined nature of proactive and self-elimination process.

V. CONCLUSIONS

In this paper we proposed a routing scheme which is well suitable for finding reliable path among devices in heterogeneous environment. The proposed routing scheme works with the efficient broadcasting technique and, a cluster based message passing method that helps in finding weak nodes to be got eliminated from the cluster so that a better communication path with better strength nodes in the path can be established. It is proved from the above analysis that our algorithm is the most efficient one, because of its proactive routing nature added with clustering and self-elimination techniques what add dynamism to the scheme. By that, the node movement, nature of the mobile environment and nature of the MAC layer are grasped by our scheme in a proactive manner. This makes our scheme to perform better in all above mentioned metrics. Next, we are supposed to make our routing scheme as a fault-tolerant one for the world of pervasive space where heterogeneous network cross layer platforms are dealt with.

REFERENCES

[01] Joe C. Chan, Doan B. Hoang, "Service Architecture For Integrating Manets With Heterogeneous Ip Networks", IEEE Communications Society / Wcnc 2005, Pp:2270-2275.

[02] Vandana Dhingra, Anita Arora, "Pervasive Computing: Paradigm For New Era Computing", First International Conference On Emerging Trends In Engineering And Technology, IEEE, 2008, Pp:349-354.

[03] Enyi Chen, Yuanchun Shi And Guangyou Xu, "A Network Service Framework For Mobile Pervasive Computing",Proceedings Of Icct200, Pp:839-845.

[04] Shin-Jer Yang And Hao-Cyun Chou, "Design Issues And Performance Analysis Of Location-Aided Hierarchical Cluster Routing On The Manet", 2009 International Conference On Communications And Mobile Computing, Pp:26-31.

[05] Biao Zhou, Zhen Cao, Mario Gerla, "Cluster-Based Inter-Domain Routing (Cidr) Protocol For Manets", IEEE 2009.

[06] Fu Yongsheng, Wang Xinyu, Li Shanping, "Performance Comparison And Analysis Of Routing strategies In Mobile Ad Hoc Networks", 2008 International Conference On Computer Science And Software Engineering, Pp:505-510.

[07] Anahita Naghshegar, Arash Dana, "Topology Control Scheme In Manets For Aodv Routing", Ictta'08.

[08] Luo Junhai, Ye Danxia, Xue Liu, And Fan Mingyu, "A Survey Of Multicast Routing Protocols For Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, Vol. 11, No. 1, First Quarter 2009, Pp:78-91.

[09] Ljubica Blazevic, Jean-Yves Le Boudec, And Silvia Giordano, "A Location-Based Routing Method For Mobile Ad Hoc Networks", IEEE Transactions On Mobile Computing, Vol. 4, No. 2, March/April 2005, Pp:97-110.

[10] Zhang Jianwu, Zou Jingyuan, Zhao Qi, "Manet Routing Protocol For Improving Routing Discovery Based On Aodv", 2009 International Conference On Networks Security, Wireless Communications And Trusted Computing, Pp:197-200.

[11] Nadir Shah, Depei Qian, Khalid Iqbal, "Performance Evaluation Of Multiple Routing Protocols Using Multiple Mobility Models For Mobile Ad Hoc Networks", Proceedings Ofthe 12th IEEE International Multitopic Conference, December 23-24,2008, Pp:243-248.

[12] N. Enneya, K. Oudidi And M. Elkoutbi, "Network Mobility In Ad Hoc Networks", Proceedings Of The International Conference On Computer And Communication Engineering 2008, Pp:969-973.

[13] Mingyang Zhang, Peter H. J. Chong, "Performance Comparison Of Flat And Cluster-Based Hierarchical Ad Hoc Routing With Entity And Group Mobility", IEEE Communications Society, Wcnc 2009.

[14] Ebrahim Mahdipour, Ehsan Aminian, Mohammad Torabi, Mehdi Zare, "Cbr Performance Evaluation Over Aodv And Dsdv In Rw Mobility Model", International Conference On Computer And Automation Engineering, 2009, Pp: 238-242.

[15] Michael S. Thompson, Scott F. Midkiff, "Experiences Using IEEE 802.11b For Service Discovery", Proceedings Of The Fourth Annual IEEE International Conference On Pervasive Computing And Communications Workshops (Percomw'06).

[16] Kamran Etemad, "Overview Of Mobile Wimax Technology And Evolution", IEEE Communications Magazine, October 2008, Pp: 31-40.

[17] Jose Luis Jodra, Maribel Vara, Jose M Cabero, Josu Bagazgoitia, "Service Discovery Mechanism Over Olsr For Mobile Ad-Hoc Networks", Proceedings Of The 20th International Conference On Advanced Information Networking And Applications (Aina'06).

[18] Aamir Saeed, Laiq Khan, Nadir Shah, Hashim Ali, "Performance Comparison Of Two Anycast Based Reactive Routing Protocols For Mobile Ad Hoc Networks", IEEE 2nd International Conference On Computer, Control And Communication, 2009. Ic4 2009.

[19] www.isi.edu/nsnam/ns/

[20] Jyotsna Rathee & Anil Kumar Verma, "Simulation and Analysis of DSDV protocol in Manets", International Journal of Information Technology and Knowledge Management, July-December 2009, Volume 2, No. 2, pp. 441-444.

[21] Pangun Park, Piergiuseppe Di Marco, Carlo Fischione, Karl Henrik Johansson,"Adaptive IEEE 802.15.4 Protocol for Reliable and Timely Communications", pp.1-18.

[22] http://www.it.uc3m.es/celeste/pdp/

[23] S. Laki *, P. Mátray, P. Hága, I. Csabai, G. Vattay, "A model based approach for improving router geolocation", Elsevier, computer networks, 2010, Pp.1490-1501.