IMPROVE QUALITY OF SERVICES IN MANETs THROUGH 3-HOP ROUTING IN CLUSTER BASED ROUTING PROTOCOL (CBRP)

Muhammad Imran Khan Khalil, Dr. Muhammad Arshad & Amer Taj

ABSTRACT

The study of Mobile Adhoc Networks (MANET's) remains attractive to achieve better performance and scalability. This study describes a clustering protocol based on 3-Hop Routing in MANETs. The protocol is an extension of cluster based routing protocol and forms 3-Hop clusters based on delay factor. Other than cluster formation delay factor is also considered in route discovery process thus incorporating QoS factor in two mechanisms. The 3-Hop clustering also helps in local repair and route shortening mechanisms as it holds comparatively more information at each node and routes can be easily repaired or shortened using this 3-Hop topology database. This delay factor is also considered in route discovery process where the routes with greater delay are avoided. The introduction of three hop routing helps in route maintenance because in three hops information at each node avoids rediscovery of route in case of route failure.

Key Words: MANETs, QoS, 3-Hop, Adhoc Networks and clustring

INTRODUCTION

Regardless of location, wireless networks can facilitate mobile users with global communication ability and the first type states simple information access. In mobile networks there are two major categories; if in networks there are fixed and wired gateways then they are infrastructured networks and the second type is infrastructureless mobile networks also called mobile adhoc networks. (Mingliang & Jinyang 1999)

Wired infrastructure is not possible in adhoc wireless networks, bandwidth and energy are the two essential factors in research areas. Inadequate bandwidth creates congestion in routing protocols. Commonly routing protocols schemes are build for wired infrastructures. They presume that the network is secure and negligible overhead for routing messages. It is important to establish wireless routing protocols that confine congestion in network. (Perkins, Royer & Das, 2001 & Broch, Maltz, Johnson & Jetcheva, 1998 & Rahman, 2004)

Mingliang et al. (1999) highlighted that nodes are divided in many disjoint or overlapping clusters in cluster based routing protocol (CBRP). Clusterhead is selected from every cluster and routing process is done by clusterhead. The communication of clusterhead should be possible through gateway nodes. There are two or more than two clusterheads as its neighbors is gateway node. Route request message is flooding in the network for routing process in cluster based routing protocol, and route request is passed between clusterheads due to less traffic in cluster based environment.

Perkins & Royer (1999) pointed out that the lack of centralization, dynamic topologies and interface characteristics are the main issues in Mobile Ad Hoc Networks (MANETs). Mobile Ad Hoc Networks require minimum bandwidth and random mobility. Routing protocols are classified in two groups for MANET

- Reactive Protocols
- Proactive Protocols

Problem Statement:

If we look into clusters in detail along with the magnitude of simplicity towards addressing and management of nodes, there exists a constant scope for improvement in different aspects of Clusters in MANETS. One such area of concern is the limited size/diameter of a Cluster, which is limited to two hops at present. We will understand the cluster and hop by examining Figure 1:

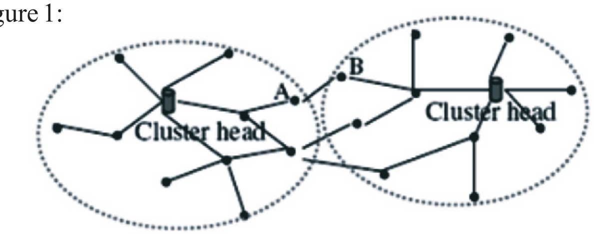

Figure 1. Network with nodes to 2 hops

Figure 1 is an illustration of two clusters existing together. To establish the routing purpose Cluster nodes are grouped together. There is direct communication within the cluster. On the other hand, communication outside the cluster is through clusterhead which is centralized node. Inside every cluster a particular node is elected as a clusterhead. Different mechanisms exist for the election of clusterhead within a cluster. Inside both clusters the clusterheads can reach the nodes at a distance not more than two hops. So the diameter and size of cluster is limited to only two hops as shown in figure 1.

The limited diameter and size of cluster introduces some drawbacks. This kind of cluster formation of two hops is not suitable for building hierarchical clusters. Moreover, performance of the clusterhead drops off due to continuous routing to another cluster. This problem is also highlighted in Cluster Based Routing Protocol (CBRP) Functional Specification. Mingliang et al. (1999). They have raised the following issue:

"Should clusters be made bigger than two hops diameter? Will the resulted more complex cluster formation and maintenance procedure offset the advantage of having a bigger size?"

Objective of this work is to increase the number of hops in a clusterhead, can reach within a cluster, to 3-hops. It intends to change the Clustering scheme 2-hop clusters to K-hop. It means that the access of clusterhead node to its members within cluster or outside the cluster is at most K hops. The number of clusterhead should be controlled by the adjustment of parameter K. Bigger K means fewer cluster heads. Figure 2 is a depiction of the same cluster environment as shown in Figure-1, but here the diameter and size of the cluster is increased to 3-hops as shown in figure 2:

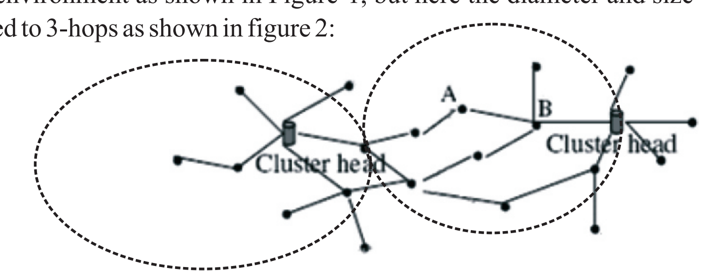

Figure 2: Network with nodes to 3 hops

LITERATURE REVIEW

Hierarchical routing linked cluster algorithm was mainly used for change in connectivity for network adaptability. This algorithm manages networks into clusters having three types of nodes: gateway nodes, ordinary node and clusterheads (Karpijoki, 2000). For the local arrangements of the nodes clusterhead is used, and the selection of the clusterhead is based on highest ID algorithm. Gateway node plays vital role in cluster through direct connection between clusterheads, and also inters cluster routing. In Linked cluster algorithm, all nodes are connected to the clusterhead. The main issue in this algorithm is cluster radius which is one hop (shigang & Lara, 1998).

Elizabeth, Royer, & Chai-Keong (1999) highlighted that, in multi-cluster and multi-hop network architecture the most common clustering scheme Lowest-ID (LID) is used according to the LID algorithm which produces cluster which are two hops in diameter. In every cluster, exactly a node, which with lower ID between his neighbors becomes a clusterhead and it supports the bunch - memberships of other member's nodes.

There are numerous routing protocols e.g. DSDV, AODV, DSR, TORA and ABR, which are used in self organized network for various functions such as: detecting and responding in network topology; broadcasting information for the construction of route, management for mobility, selection and construction of routes, and traffic forwarding in the defined routes (Ying, LiuYong & Shi, 2000)

.The routing function of Destination-Sequenced Distance-Vector (DSDV) is same as Distributed Bellman-Ford (DBF) algorithm. In DSDV routing protocol the host node advertise the view of the network structure to other host nodes to keep its information regarding the network periodically. Every host node maintains the routing table which holds the accessible target nodes and number of hops. (Charles & Pravin, 1994)

Ad hoc On-Demand Distance Vector (AODV) is a routing protocol which is mostly used for mobile ad hoc networks and for mobile routing. AODV develops their routes on the basis of Destination-Sequenced Distance-Vector algorithm. The main difference between these two protocols is; AODV is reactive protocol which means it maintains a route list when needed and DSDV is proactive protocol. Another important feature in AODV is to support the multicast routing (Charles & Elizabeth, 1998)

Another protocol which is used for wireless is Dynamic Source Routing (DSR) which uses source routing instead of hop by hop, because every packet holds the order detail of host nodes due to which packet passes. The key feature of this routing protocol is that; there is no need to hold latest routing information for forwarding the packets for intermediary nodes, the advantage of this feature is reduction of bandwidth, full utilization of route cache, discovering of shorter route for nodes, handling of errors and maximum utilization of battery power. DSR has two main components: discovery of routes and route maintenance (Josh, David & David, 1998)

For distributed routing the Temporally Ordered Routing Algorithm (TORA) is used which is highly adaptive and loop free, the main concept behind this protocol is link reversal. The main idea for designing the TORA is message controlling and localization of small set of nodes due to which it presents several routes for a destination. TORA has three main components: creation of routes, maintenance of routes and final is removal of unnecessary routes (Park & Corson, 1998)

Ying, LiuYong & Shi, (2000) after reviewing the different routing protocols say that there are a lot of queries which play an important role for the designing of routing protocols for self organized network, such as

- Routing Architecture
- Unidirectional links support
- Usage of super hosts
- Quality of Services routing
- Multicast support

PROPOSED SCHEME

In this research taking CBRP from 2 hops to 3 hops routing is based on some changes in its basic functionality; mostly changes in packet formats.

Cluster Formation:

When an undecided node comes in range of some cluster(s), it sends HELLO (solicitation) message to its immediate neighbors. It sends this message multiple times within a specific time period; if time expires and reply isn't received, it declares itself as a cluster head and broadcasts HELLO message; telling its neighbors of its new role. On the other hand if it receives cluster advertisement message, the node will examine the hop count value in reply to its messages and if it is less than or equal to 3 then the node will become a part of a cluster which has less hops towards clusterhead and then it will send cluster acceptance message. The following flowchart describes the steps involved in cluster formation.

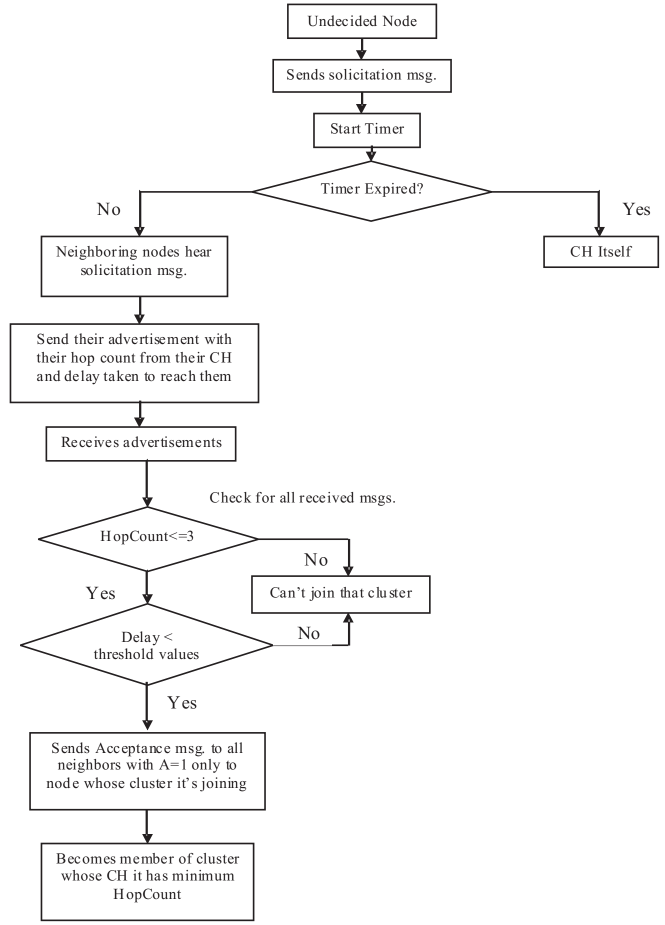

Figure 3. Formation of Cluster in CBRP

To explain this concept we look at the following figure 4 and explanation:

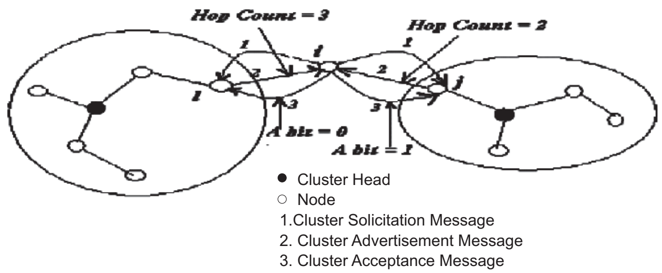

Figure 4. Cluster Formation Process

Cluster Formation process thus consists of exchange of three types of messages:

i. Cluster Solicitation Message
ii. Cluster advertisement Message
iii. Cluster Acceptance Message

And they will now be discussed with the help of the diagram shown above

Cluster Solicitation Message

A node i wants to become a member of any cluster which presently doesn't belong to any cluster then it will send cluster solicitation message to their neighbors (nearest clusters). This message contains its ID other than the type of the message as shown in figure 5.

100	**NodeID**

Figure 5. Cluster Solicitation Message

100 - CBRP packet type indicating it's SOLICITATION message.

Cluster Advertisement Message:

Cluster solicitation message received by node j and l and then these nodes send advertisement message as shown in figure 6 bellow:

101	**HopCount**	**CH_ID**	**Delay**

Figure 6. Cluster Advertisement Message

101 - CBRP packet type for ADVERTISMENET message:

The above figure demonstrates the cluster advertisement message in node j and l which hold different information such as CH_ID (clusterhead identification) of related cluster. HopCount contains the information about number of hops in which the node i will remain from the clusterhead. Delay contains the information regarding delay in milliseconds from the clusterhead. Every node for example node j to i holds estimated hop count in the cluster advertisement message which is 2 hops as shown in the above figure, same is the hop count from node l to I which is 3 hop.

Cluster Acceptance Message:

Node i checks the value of hop count in cluster advertisement message less than or equal to 3 after the reception of cluster advertisement. If this condition is satisfied, it checks for delay value. The delay value received also must be less than a threshold value. The reason

is the bad link i.e. with greater delay should not be considered in the beginning, so delay can be avoided later on. If the HopCount and Delay is more than the threshold value after that new node will choose the clusterhead with the minimum HopCount and will send cluster acceptance message to nodes whose advertisement message(s) have been received as shown in figure 7.

110	**A**	**G**	**NodeID**

Figure 7. Cluster Acceptance Message

110 - CBRP packet for ACCEPTANCE message:

Cluster acceptance message contains different information such as A indicates the acceptance of advertisement message. The lowest ID algorithm is used when HopCount value is same in 2 or more than two cluster advertisement messages. G indicates cluster gateway, a node declares itself as gateway node when it receives two or more than two cluster advertisement messages from nodes which belong to different clusters. After some specific time period node i declares itself as a clusterhead when it doesn't receive cluster advertisement message after sending cluster solicitation or node i receives all messages with higher HopCount and higher delay.

HELLO Messages:

Once a node joins a cluster or becomes a clusterhead itself, it broadcasts periodic HELLO messages to all its neighboring nodes, telling them about its neighbors and adjacent CHs. Thus we can say that HELLO message consists of:

- Neighbor Table
- Cluster Adjacency Table(CAT) formed through adjacent cluster discovery

After receiving Hello messages each node updates both the neighbor table and CAT it maintains.

We will consider figure 8 to understand the structure of Neighbor table and cluster adjacency table.

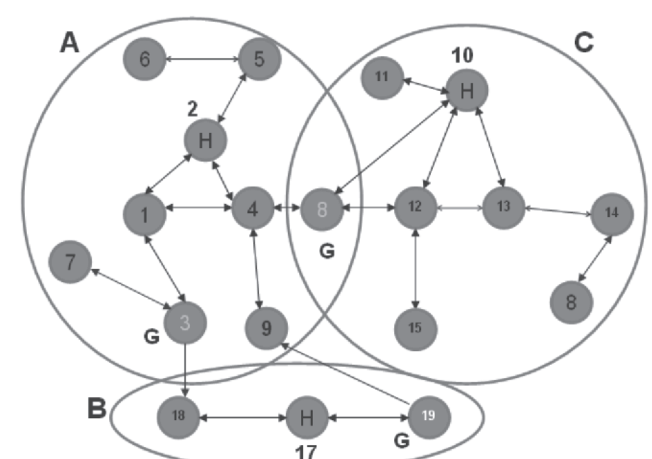

Figure 8. overlapped Clusters

Neighbor Table

Neighbor table is an abstract data structure which is employed for link status sensing and storing other important information. Every table entry consists of:

1. Neighbor IDs: Node identification number which has connectivity with
2. Link Status: link status either bi-directional or uni-directional
3. Role: Neighbor role either clusterhead or a member
4. Map Count: Hop count from itself to its neighbor
5. Delay: Delay in seconds from itself to neighbor

Neighbor ID's	Link Status	Role	Hop Count	Delay
2	Bi Directional	Cluster Head	1	0.5
3	Bi Directional	Member	1	4
4	Bi Directional	Member	1	1.5
5	Bi Directional	Member	2	2
7	Bi Directional	Member	2	1.9
8	Bi Directional	Member	2	4
9	Bi Directional	Member	2	3
6	Bi Directional	Member	3	3.5

Figure 9 Neighbor Table

Cluster Adjacency Table and Adjacent Cluster Discovery

The discovery of its neighboring clusters is the main objective of Adjacent Cluster Discovery. Each node maintains all the information of their adjacent clusterheads and records that information in cluster adjacency table. Adjacent clusterheads will be 3 hops away for the member nodes and its discovery can be through the reception of Hello messages. The Hop Count could be 3 or 4 for neighboring clusterheads. To discover the clusterheads 3 hops away a clusterhead only uses the HELLO messages as shown in figure 10.

Adj. Clusterhead ID	Gateway
2	2
17	3
10	8

Figure 10. Cluster Adjacency Table

The communication of two or more clusterheads is done by the gateway node and it is the member of adjacent or neighbor cluster, for this purpose the gateway field in CAT keeps the record of all those nodes which play the role of gateway. CAT is updated through the HELLO messages by node which is exactly 3 hops away. Every node broadcasts its summarized cluster adjacency table information as a cluster adjacency extension in HELLO message to its clusterhead as shown in figure 11.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
																Length															
L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
Adjacent Cluster Head [1] Address																															
…………																															
Adjacent Cluster Head [Length] Address																															

Figure 11. Cluster Adjacency Extension to HELLO message

Length: Total clusterheads which are listed in extension
L: L field identified for clusterhead link status.
LINK_BIDIRECTIONAL: At least one gateway and bi-directional link .
or else, LINK_FROM.
0 --- LINK_BIDIRECTIONAL
1 --- LINK_FROM

After considering neighbor table and CAT we now look at the Format of HELLO message for route communication as shown in figure 12:

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
															1	1	1	CLength						Length						S	
L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R	L	R
Neighbour[1]Address																															
HopCount[1]																Delay[1]															
………………																															
Neighbour [Length] Address																															
HopCount[Length]																Delay[Length]															
Adjacent Cluster Head [1] Address																Gateway [1]															
……………………																……………………															
Adjacent Cluster Head [CLength] Address																Gateway [CLength]															

Figure 12. HELLO message packet format

111 CBRP packet for Hello message
Length Number of neighbors listed
S Status of sender
0 – Undecided
1 – Cluster Head
2 – Cluster Member
L Link Status
0 – Bidirectional
1 – Cluster Head
HopCount Numbers of Hops from neighbor to itself
Delay Node it takes

3 Hop Routing:

i. Route Discovery
a. RREQ
b. RREP
ii. Packet Forwarding
iii. Route Shortening
iv. Local Repair
v. Route Error

Route Discovery:

It is the system used by a node which wishes to propagate data packet to its destination node and requires to obtain route from this node to destination D i.e. source route to destination.

a. Route Request

To find source route, RREQ message is flooded in clusters.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td>0</td><td>1</td><td>0</td><td colspan="7">Num1</td><td colspan="7">Num2</td><td colspan="15">Identification</td></tr>
<tr><td colspan="32">DELAY (time in milliseconds)</td></tr>
<tr><td colspan="32">Target Address</td></tr>
<tr><td colspan="32">Gateway Node Address[1]</td></tr>
<tr><td colspan="32">Neighbouring Cluster Head[1]</td></tr>
<tr><td colspan="32">…….</td></tr>
<tr><td colspan="32">Gateway Node Address[Num1]</td></tr>
<tr><td colspan="32">Neighbouring Cluster Head[Num1]</td></tr>
<tr><td colspan="32">Cluster Address[1]</td></tr>
<tr><td colspan="32">……….</td></tr>
<tr><td colspan="32">Cluster Address[Num2]</td></tr>
</table>

Figure 13. RREQ packet format

010	Cluster Based Routing Protocol Route Request packet type
Num1	Total Gateway and Adjacent node addresses
Num2	Total addresses for clusters
Identification	The number for identification has been taken from correspondent Route request
Gateway Node Address	Which propagates the route request
Neighboring clusterhead:	The correspondent clusterhead whose route request is forwarded to gateway node

Route request (RREQ) sends out along with target node D by source node S. RREQ fill up with neighboring clusterhead, adjacent clusterhead and host clusterhead entries, correspondent gateway node address is host clusterhead or adjacent cluster(s) gateway. Preliminary route request is broadcast. RREQ is forwarded only once by each clusterhead and is not forwarded again to that node which is already in the route. Delay field contains time in seconds taken to reach from one hop to another and is incremented automatically i.e. the delay taken from one node to next is added to the previous value in this field, refer to figure 13.

When a node N receives a RREQ it does the following:

```
IF N is member
IF D is in the neighbor table
send RREQ to D
ELSE IF N is gateway to Clusterhead C
forward RREQ to C
ELSE
```



```
discard RREQ
ENDIF
ELSE IF N is Clusterhead
IF RREQ already seen
discard RREQ
ELSE
record ID in cluster address list of RREQ
IF D is neighbor OR D is three hops away
send RREQ to D
ELSE
FOR EACH neighboring Clusterhead C DO
IF NOT C in address list of RREQ
record C in cluster address list of RREQ
ENDIF
ENDFOR
ENDIF
broadcast RREQ
ENDIF
ENDIF
```

To understand it consider the following flowchart

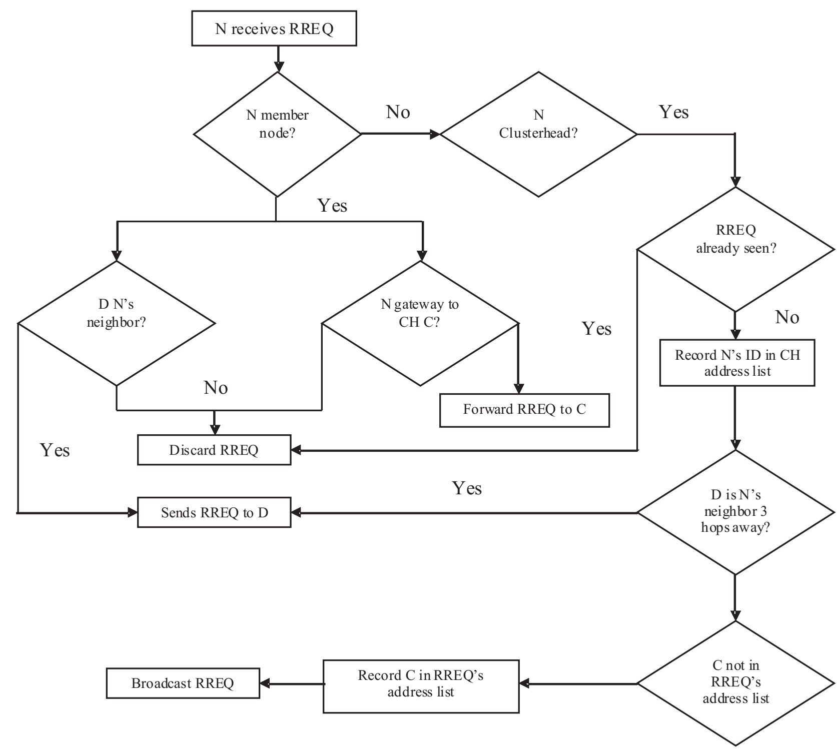

Figure 14. Route Request

© 2012 CURJ, CUSIT

b. Route Reply:

Destination after receiving first RREQ waits for a specific time period to receive other route requests with the same sequence number When the time is over it compares all delay fields of the received route request and propagates a reply packet called route reply to source through the route whose delay was minimum as shown in figure 15.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

0	0	1	Num1	G	Num2	Identification
Cluster Address[1]						
....						
Cluster Address[Num1]						
Calculated Route[1]						
....						
Calculated Route[Num2]						

Figure 15. RREP packet format

001	Cluster based routing protocol route reply packet type
G	G is the indication of route reply which has unnecessary packet of reply
Identification	The number for identification has been taken from correspondent Route request
Num1	Total addresses of cluster
Num2	Total addresses of estimated route
Cluster Address	Total number of cluster addresses has been taken correspondent Route request
Calculated Route	The order of addresses hop to hop estimated by clusterhead

Route Reply (RREP) holds all the information of cluster addresses, which give the information regarding sequences of clusters route reply, which must traverse to reach source node. Every clusterhead has the knowledge to reach its adjacent or neighboring clusterheads as shown in figure 15.

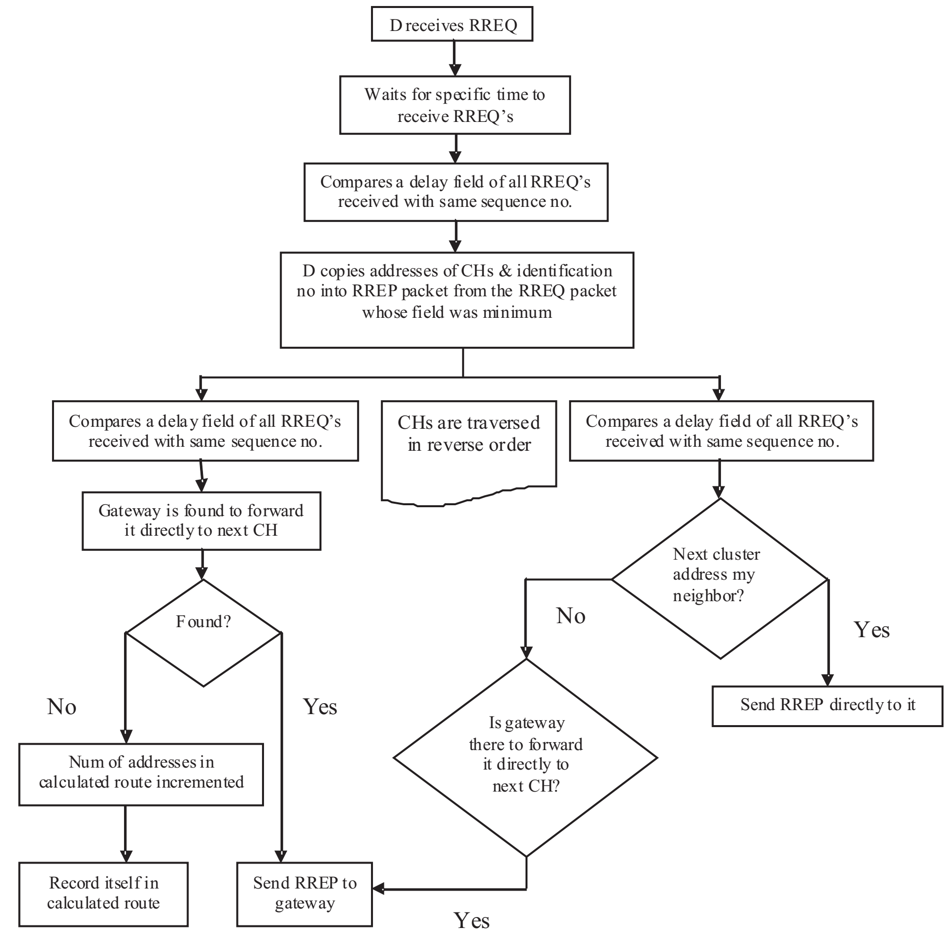

Figure 15. Route Reply from Destination to Source

Packet Forwarding

The data packet to be forwarded contains all the addresses that have to be traversed in order to reach destination along with the node currently being accessed and bits indicating route has been shortened or has been salvaged using local repair. The format of the packet is shown as figure 16.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

	0	0	0	Num	R	S	Current Num
Address[1]							
....							
Address[Num]							

Figure 16. Routing packet format

000	Cluster based Routing Protocol packet category
Num	Total addresses exist in source route

Current Num Identify the presently visited route
R Flag Identify the route which has been retrieved through local repair method
S Flag Identify the route which has been condensed

Route Shortening

For route shortening the 3-hops topology database information will be used to shorten sub-optimal route. On the reception of source routed data packet by node it will further find out the node in the defined route which unvisited to its neighbor nodes. Before forwarding the packet, it sets S flag and accordingly shortens the source route if it succeeds. It sends back a gratuitous Route Reply on the reception of destination node with data packet along S flag set as shown in figure 17.

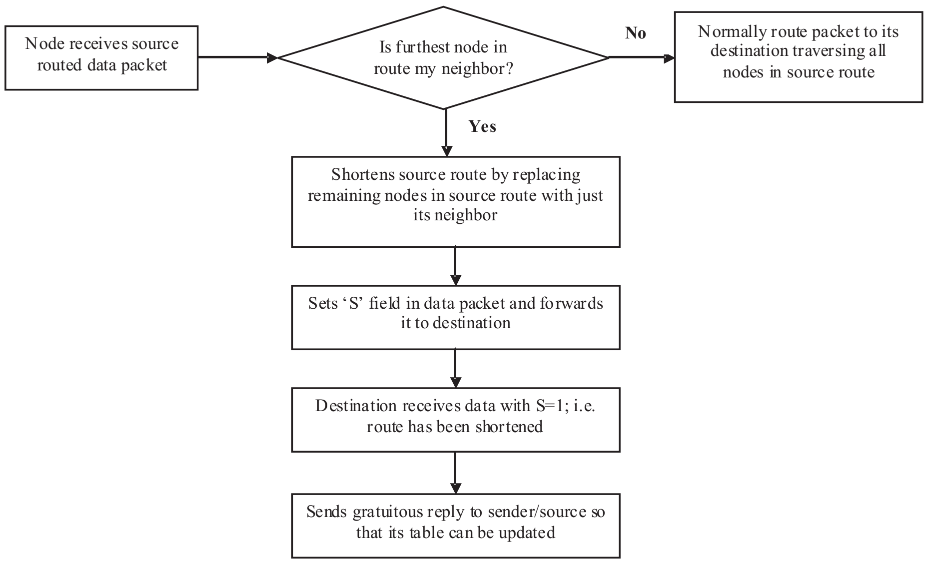

Figure 17. Flowchart for Route Shortening Procedure

Local Repair

On the reception of broken link forwarding node strives to repair the route on the basis of its local knowledge.

a. In the local repair mechanism, if the hop is accessible in the source route via node which is specified to the coming hop by its 3 hop topology database.
b. The second checking is regarding inaccessible coming hop that can be accessed intermediary node by its 3 hop topology database.
c. And finally if packet can be saved, it should be modified source route and it sets the R flag and delivery of the packet to new hop.

Route Error

On the reception of the coming hop with source route by forwarding node which is not further accessible i.e. the local repair mechanism has failed. After that it should create a packet of route error and propagate it to source for link failure as shown in figure 18.

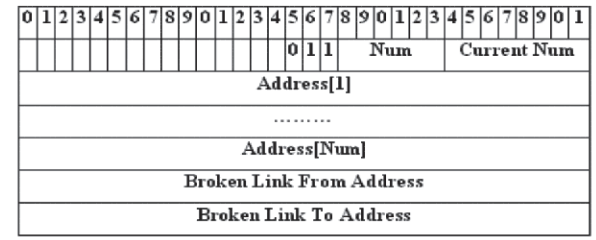

Figure 18. Route Error Packet

011 clusters based routing protocol packet delivery type
Num Total addresses
Address Source to destination route addresses
From Address Error packet own address
To address inaccessible coming hop address

When the source route will receive the error packet it will reinitiate the route discovery process to find destination.

CONCLUSION & FUTURE WORK

In this research the main focus is on cluster-based routing protocol (CBRP) proposed earlier but few changes in its cluster formation, route discovery and route maintenance mechanisms are discussed in detail. The clusters are formed of 3 hop radius by exchanging solicitation, advertisement and acceptance messages and considering delay factor in joining a cluster that affects data transmission later. This delay factor is also considered in route discovery process where the route with greater delay is avoided. The introduction of 3 hop routing helps in route maintenance because three hop information at each node avoids rediscovery of route in case of route failure. So, clusters can be made bigger than two hop diameter and the new complex methodologies for cluster formation and route maintenance do not offset the advantage of having a bigger size rather decrease network traffic and routing overhead.

Simulation experiments can be done with different scenarios of the cluster formation and route maintenance phases as part of future work

REFERENCES

Broch, J., Maltz, D., Johnson, D., Hu, Y. & Jetcheva, J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. 4th international Conference on Mobile Computing and Networking .

Chai-Keong, T. (1997). Associativity-Based Routing for Adhoc Mobile Networks. Wireless Personal Communication , 4 (2), 103-139.

Charles, E. & Elizabeth, M. (1998). Ad-Hoc On-Demand Distance Vector Routing. Retrieved from IEFT Tools: http://tools.ietf.org/html/draft-ietf-manet-aodv-02

Charles, E. & Pravin, B. (1994). Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers. Proceedings of SIGCOMM'94 Conference on Communication Architectures, Protocols and Application, (pp. 234-244).

Corson, S. & Macker, J. (1999). Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration. Retrieved from IEFT Tools: http://www.ietf.org/rfc/rfc2501.txt

Eli, G. & Dimitri, B. (1981). Distributed algorithms for generating loop-free routes in networks with frequently changing topology. IEEE Transaction Communication .

Elizabeth, M., Royer & Chai-Keong, T. (1999). A Review of Current Routing Protocols for Ad Hoc Mobile wireless Networks. IEEE Personal Communication , 6 (2), 46-55.

Joseph, M. & M-Scott, C. (1998). Mobile Ad Hoc networking and the IETF. ACM SIGMOBILE Mobile Computing and Communications review , 2 (4).

Josh, B., David, J. & David, M. (1998). The Dynamic Source Routing Protocol for Mobile Ad Hoc Network. Retrieved from IEFT Tools: http://tools.ietf.org/html/draft-ietf-manet-dsr-01

Karpijoki, V. (2000). Signaling and routing security in mobile and ad-hoc networks. Retrieved from Telecommunications Software and Multimedia Laboratory: http://users.tkk.fi/vkarpijo/netsec00/netsec00_manet_sec.pdf

Leiner, B., Nielson, D. & Tobagi, F. (1987). Special issue on packet radio network design. Proceeding of IEEE , 75 (1), 6-20.

Mingliang, J., Jinyang, L. & Y, C. (1999). Cluster based routing protocol (CBRP). Retrieved from IETF Tools: http://tools.ietf.org/html/draft-ietf-manet-cbrp-spec-01

Park, V. & Corson, S. (1998). Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification. Retrieved from IEFT Tools: http://tools.ietf.org/html/draft-ietf-manet-tora-spec-01

Perkins, C. & Royer, E. (1999). Ad-hoc on demand distance vector routing. Proceedings 2nd IEEE workshop on Mobile Computing systems and applications, (pp. 90-100).

Perkins, C., Royer, E. & Das, S. (2001). Ad hoc On-Demand Distance Vector AODV Routing. Retrieved from IETF Tools: http://tools.ietf.org/html/draft-ietf-manet-aodv-08

Rahman, A. (2004). Security issues in mobile systems. Retrieved from http://www.cs.ucl.ac.uk/staff/F.AbdulRahman/Docs/Sec-in-ob.html

Shigang, C. & Llara, N. (1998). An overview of Quality of Service Routing for Next Generation High-Speed Networks: Problems and Solutions. IEEE Network Magazine , 12 (6), 64-79.

Ying, C., Lv, Q., LiuYong & Shi, M. (2000). Routing protocols overview and Design Issues for Self-Organized Network. Communication Technology Proceedings, 2000. WCC - ICCT 2000. International Conference on, 2, pp. 1298-1303.

Muhammad Imran Khan Khalil: Lecturer at department of Computer Science & Information Technology, University of Engineering and Technology, Peshawar, Pakistan. MS in Information Technology and Project Management. Over 10 years of teaching and research experience. Areas of interest are Computer Network, software Engineering, Management information System, and Project Management.
Email : imrankhalil79@gmail.com

Dr. Muhammad Arshad: Assistant Professor, Department of Computer Science, City University of Science & Information Technology, Peshawar, Pakistan. Ph.D in Computer Science from Liverpool John Moores University, Liverpool UK and he has more than 8 years of experience in research and academics. He has more than 12 research publications and his area of expertise are Peer-to-Peer networks, networked appliances, Quality of Service, Network Security, Web Services and Home Network.
e-mail: m.arshad@cusit.edu.pk

Amer Taj: Lecturer at department of Computer Science & Information Technology, University of Engineering and Technology, Peshawar, Pakistan. More then six years teaching experience. Area of interest: Digital Communication System, Digital Logic and Design, and Computer Networks
e-mail: amertaj321@gmail.com