Available online at www.worldscientificnews.com

World Scientific News

WSN 45(2) (2016) 252-263 EISSN 2392-2192

Analyze the Performance of Routing Protocols in Clustered Ad Hoc Networks: A Survey

T. Parameswaran[1], Dr. C. Palanisamy[2], P. Bhagya devi[3,*]

[1]Teaching Fellow, Department of CSE, Anna University Regional Centre, Coimbatore, India

[2]Professor and Head of the Department of IT, Bannari Amman Institute Of Technology, Sathyamangalam, Erode, India

[3]PG Scholar, Department of CSE, Anna University Regional Centre, Coimbatore, India

*E-mail address: bhagya3devi@gmail.com

ABSTRACT

A Mobile ad hoc network is a continuously self-forming, infrastructure-less network of mobile devices connected without wire. Routing protocols for Mobile ad hoc network are responsible for maintaining the routes in the network and have to ensure the reliable multi-hop communication. Many existing routing protocol approaches measures the performance of ad hoc networks. In ad hoc network faces some challenges like Qos, network congestion, data collision. Using clustering in MANET to avoid packet transmission delay, network congestion and packet loss, etc. This paper aims to provide a comprehensive study of the routing protocol performance in clustered ad hoc network.

***Keywords*:** MANET; Clustering; Routing Protocol; Quality of Service; Clustering algorithms

I. INTRODUCTION

Ad hoc network is an autonomous system node connected with wireless link. The node in the ad-hoc network communicates with other node without any physical illustration. The nodes in the ad- hoc organization instantly form the network whenever the communication is recognized [9]. Each node in the network communicates with other node using radio waves.

The entire network is distributed and nodes are collaborating with each other without fixed station access point (AP) or base station. An ad- hoc network is a local area network that builds an automatic connection between the nodes in the network. The ad hoc networks can be classified depending on their applications such as Mobile Ad hoc NETwork (MANET) which is a self-forming infrastructure less network of mobile devices communicated through wireless link. Vehicular Ad hoc NETwork (VANET) uses travelling vehicles as nodes in a network to create a mobile network. Wireless Sensor Network (WSN) consists of independent sensors to control the environmental actions.

The advantages of an ad hoc network

Separation from central network supervision, Self-configuring nodes are also routers, Self-healing through continuous re-configuration, Scalability incorporate the adding of more nodes, Mobility allows ad hoc networks created on the fly in any situation where there were multiple wireless devices, stretchy ad hoc can be temporarily setup at anytime, in any place, Lower getting in progress costs due to decentralized supervision, The nodes in ad hoc network need not rely on some hardware and software. So, it can be coupled and communicated quickly.

The ad hoc networks are self-forming, self-maintain, self-curing architecture. It faces some challenges are, no fixed access point, dynamic network topology, contrary environment and asymmetrical connectivity [14]. Ad hoc network instantaneously forms and accommodate the modification and limited power. Finally, ad hoc has no trusted centralized authority. Due to the dynamic changing property, the *ad hoc faces some challenges such as,*

Quality of Service (Qos)

The ad hoc network is excitedly creating the association whenever the node wants to communicate with their neighbor node. Suitable the dynamic shifting topology in ad hoc network, providing Qos is a tedious task [3]. Qos are essential because of quick development in mobile technology and existent time applications like multimedia, voice. Providing Qos in ad hoc network is necessary to keep up finest-effort-of service. The Qos metric are bandwidth, latency, jitter and delivery assurance. The bandwidth is used to indicate the data rate carried in the network. Latency ensures the delay occurs from basis to target. Jitter indicates the variant of delay. Reliability demonstrate the percentage of deny to access the network service. Wireless channels are changeable quickly and it severely affects the multi-hop flows. In ad hoc networks, the peer-to-peer channel quality alters quickly. So, the link quality may be affecting the peer-to-peer Qos metrics in the multi-hop path.

Scalability

The scalability crisis occurs in ad hoc networks appropriate to the nature of the multi-hop. The scalability in ad hoc network depends on the network range and forwarded package capacity in the network. Recently, lot of troubles address in large-scaled ad hoc networks.

Performance measurement of ad hoc network

Internet Engineering Task Force (IETF) identified the performance metrics of the ad hoc network based on their activities. The performances of ad hoc networks based on the network capability, network connectivity, topological alteration rate, link rate and mobility

[5]. The ad hoc network performance measurement is based on the following metrics like Packet transmission ratio, Route procurement, Routing overhead.

Cooperation between nodes

Cooperation between the nodes is important in ad hoc network. Each node in the network cooperates with other node for packet forwarding and routing.

Security

Security is a major concern in the ad hoc networking standards. Data transformation in ad hoc network should be completed in a secured way [16]. The security issues in ad hoc network are dynamic topology, bandwidth, and small device size and restricted battery life. Due to the dynamic nature, it is difficult to maintain secured transmission in the network. The ad hoc network does not depend on any pre-existing infrastructure so that the node can exit and enter the network in any situation where security may fall down. Two types of attacks occurred in ad hoc network, first is be a passive attack; this passive attack does not change the transmitted data in the network. But, it can endure unauthorized user to find the message. Second, is active attack, it is a severe attack and prevents the message transfer between the node in the network. It may allow the unauthorized user to modify the message. The malicious node can be recognized by dropped package, battery drained, bandwidth consumption, unreliable packets, delay, connection break and false routing. So to overcome those challenges to use clustering in ad hoc network, clustering techniques used in MANET.

II. CLUSTERING

Clustering become applied in a variety of fields, ranging from engineering (machine learning, artificial intelligence, pattern recognition, mechanical engineering) computer sciences (web mining, image segmentation, etc.) life and medical sciences, earth sciences, social sciences and economics. Clustering algorithms developed to solve a particular problem, in a specialized field [2]. Also monitor the routing protocol performance.

To use clustering technique to analyze the performance of the routing protocols. Routing protocols used to discover the routes from source to destination. There are many cluster formation algorithm will be present. Each has a specific character like mobility, connectivity, identity, etc.

Classification of clustering algorithms

In self-association schemes, CH is a node that consumes more energy than cluster members when they involve in aggregating, processing and routing data. Clustering algorithm is a heuristic in nature and NP hard [11]. Distributed clustering algorithms are more feasible algorithm compared to mainly use clustering algorithms. Only distributed clustering algorithms therefore are considered in that analysis.

Generally these algorithms are coming under static clustering algorithms and do not change the CHs once should selected. However, the energy efficiency is not a primary objective of most of the Identity-based clustering algorithms. A load balancing heuristic will be added to these algorithms and hence, longer, low variance CH durations can be achieved.

In neighborhood information based clustering algorithms; sensors should have information about their neighbors and should be able to choose a number of neighbors within a pre-specified transmission rate (cluster rate). Based on the connectivity-based heuristics considered a number of neighbors, some algorithms select sensors with maximum number of one-hop neighbors as the CHs. Some other algorithms under that conditions use a combination of metrics in addition to node degree such as: transmission power; mobility; and the remaining energy of the nodes. Depending on specific application, selected or all of these parameters will be utilize for CH selection. The power consumption of the CHs can be reduced by using load balancing heuristic in the algorithms.

This may further build a larger number of clusters within the network create jamming in data routing to a base station. Re-clustering or CH re-selection is not considered in these algorithms and mostly they are static clustering algorithms [17]. In Probabilistic clustering algorithm, a past probability assigned to each sensor node is used to identify the CHs. The probabilities are assigned to individual node in the cluster to facilitate individual node to decide on their selection of a CH in the cluster while considering few other prime parameters. In adding together to the probability assigned to each node, residual energy at each nodes or node degree is taken as the primary parameter to select CH. Clustering algorithms in this category shows faster convergence in addition to energy efficient network utilization, efficient load balancing and low message overheads. Recently proposed biologically inspired clustering algorithms consume swarm intelligence techniques which model the joint behavior of social insects like ants. These algorithms are not yet matured and improvements are to be required.

In these clustering algorithms, colonial closure model which have been derived based on ant colonies are used. Biologically inspired clustering algorithms should be shows that they can dynamically control the CH selection while achieving uniform distribution of CHs and optimal number of clusters [10]. Now provide an overview of the clustering algorithms that are most commonly considered when investing the self-association of WSNs.

IDENTIFIER-BASED CLUSTERING

A unique ID is assigned for the each node. Nodes know the IDs of its neighbors and cluster head is chosen following some certain rules as given below [13].

Lowest ID cluster algorithm (LIC) is an algorithm in which a node with the minimum id is selected as a cluster head. Thus, the ids of the neighbors of the cluster head will be higher than the cluster head [18]. A node is called as gateway if it is lies within the transmission range of two or more cluster heads.

Max-Min d-cluster formation algorithm **generalizes** the cluster definition to a assortment of nodes that are up to d-hops away from a cluster head. Due to the large number of nodes are involved, it is desirable to let the nodes operate asynchronously. The clock synchronization overhead is avoided for providing additional processing savings.

CONNECTIVITY-BASED CLUSTERING

Highest connectivity clustering algorithm (HCC) The degree of a node is computed based on its space from others. Each node broadcasts its id to the nodes that are within its communication range. The node with maximum number of neighbors (i.e., maximum degree)

is choosing based a cluster head [20]. The neighbors of a cluster head are members of the cluster and can no longer participate in the part of the selection process. Since no cluster heads are directly connected, only one cluster head is allowed as per the cluster. Any two nodes in a cluster are at most two-hops absent since the cluster head is directly connected to each of its neighbors in the cluster. Fundamentally, each node either becomes a cluster head or remains a normally node [13].

K-hop connectivity ID clustering algorithm (KCONID) combines two clustering algorithms: the Lowest- ID and the Highest-degree heuristics. In order to select cluster heads connectivity is considered as a first criterion and lower ID as a secondary criterion. Using only node connectivity as a criterion causes numerous ties between nodes On the other hand, using only a lower ID criterion generates more clusters than necessary. The purpose is to minimize the number of clusters formed in the network and in this way obtain dominating sets of smaller sizes. Clusters in the KCONID approach are formed by a cluster head and all nodes that are at distance at most k-hops from the cluster head.

MOBILITY-AWARE CLUSTERING

Mobility-based d-hop clustering algorithm partition an ad hoc networks into d-hop clusters based on mobility matrices. The objective of form a d-hop cluster is to make the cluster diameter more flexible. This algorithm is based on the mobility matrices and the diameter of a cluster is adaptable with respect to the node mobility. This clustering algorithm assumes that each node can measure its received signal strength. In this manner, a node can calculate approximately its distance from its neighbors [13].

Mobility-based Frame Work for Adaptive clustering partitions a number of mobile nodes into multi-hop clusters based on (a, t) criterion. The (a, t) criterion indicates that every mobile nodes in a cluster has a path to every other node that will be available over some time period ‘t’ with a probability ‘a’ despite of the hop distance between them. Cluster framework is based on an adaptive architecture designed to dynamically organize mobile nodes into clusters in which the probability of path availability can be bounded, and the impact of the routing overhead can be effectively managed. The cluster organization supports an adaptive hybrid routing strategies that is more responsive and effective when node mobility is low and more efficient when node mobility is high. The purpose of this strategy is to supports more scalable routing infrastructure that is able to adapt to high rates of topological change. This is achieved by using prediction of the future state of the network connections in order to provide a quantitative bound on the availability of paths to cluster destinations. A metric which captures the dynamics of node mobility, makes the scheme adaptive with respect to the node mobility.

LOW COST OF MAINTENANCE CLUSTERING

Least cluster change algorithm (LCC) is a considerable improvement over LIC and HCC algorithms as for as the cost of cluster maintenance has considered. Most of protocols are executes the clustering procedure sporadically, and re-cluster the nodes from time to time in order to satisfies some specific characteristics of the cluster heads. In HCC, the clustering scheme has performed periodically to ensure the “local highest node degree” aspects of a cluster head. When a cluster head finds member nodes with a higher degree, it is forced to hand over its cluster head role. This mechanisms, involves frequent re-clustering. In LCC the

clustering algorithm is divided into two steps: Cluster formation and Cluster maintenance. The cluster formation is simply follows LIC, i.e. from the beginning mobile nodes with the lowest ID in their neighborhoods are selected as cluster heads. Re-clustering is a event-driven and invoked in only two cases:

1. When two cluster heads moves into the reach range of each others, one gives up the cluster head role.
2. When mobile nodes cannot access any cluster head, it rebuilds the cluster structure for the networks according to LIC.

Hence, LCC significantly improves the cluster stability by relinquishing the requirements that a cluster head should have some special features in its local area. But the second case of the re-clustering in LCC indicates that a single node's movement still invokes the complete cluster structure re-computation and thus results in large communication overhead.

Adaptive clustering for mobile wireless network ensures a small communication overhead for building a cluster as each mobile node broadcasts only one message to the cluster construction. In this adaptive clustering method, every mobile node i keeps it own ID and the ID of its direct neighbors in a set Gi. Each and every mobile node with the lowest ID in their local area declares to be a cluster head and set its own ID as its cluster ID (CID). The CID information including such as a mobile node's ID and CID. When a mobile node i receives CID information from a neighbor j, it deletes j from its set Gi. If the CID information from j is a cluster head maintain, the mobile node checks its own CID feature. If its CID is unspecified (it is not involved in any cluster yet) or larger than the ID (CID) of j, it sets j as it's a cluster head. The processes continue until all mobile nodes access some cluster. After cluster formation has completed, cluster heads are no longer used in any further cluster maintenance period. In the maintenance period, when a mobile node i find out that the distance between itself and some node j in the same cluster become greater than 2-hop, it invokes a cluster maintenance mechanisms. If node i has a direct neighbor of the node with the highest intra-cluster connectivity in its cluster, it remains in the cluster and remove a node j; otherwise, it joins as a neighboring cluster. As soon as there is no proper cluster to join, it forms a new cluster to wrap itself. Since these mechanisms likely forms a new cluster but without any cluster elimination or merge mechanisms, the cluster size is decreases and the number of clusters increases as time advances [17]. Eventually, almost every mobile nodes forms a single-node cluster, and the cluster structure disappear.

III. ROUTING PROTOCOL

Mobile ad hoc networks are characterized by multi-hop network topologies that can be change frequently due to the mobility; efficient routing protocols are needed to establish the communication paths between the nodes, without causing excessive control traffic overhead or computational overloads on the power constrained devices. Some of the solutions are subjected to standard isolation within the IETF. Routing protocols for ad hoc networks are generally classified as reactive and proactive. Reactive protocols, also called on-demand protocols, discover routes only when they are needed. Proactive routing protocols store a table

with routes to all nodes in the network at each node [6]. The goals of routing protocols are: Find shortest path, Decrease routing-related overhead, Find stable routes.

Routing protocols for ad hoc networks are generally classified as reactive and proactive. Reactive protocols are also called as on-demand protocols, its discover the routes only when they are needed. When nodes have packets to send and there is no route to the destination, the node starts a route discovery process by flooding the network with a inquiry. A route is created either when the destination node or an intermediate node, responds to the inquiry. Since packets must be wait in a buffer while the route is being encountered, the delays experienced by initial packets increase. Regardless of this increase, however, the reactive schemes are demand fewer resources since the routing tables store only the set of routes needed by the node. Reactive protocols are demands a certain amount of bandwidth for the detection process, however the Proactive routing protocols store a table with routes to all other nodes in the network at each node. Routing tables are built and updated by exchanging periodic control messages between the nodes [7]. A node that has a packet to send only needed to finds the corresponding entry in the routing table. Proactive schemes demand more bandwidth than reactive schemes, since the nodes need to send the periodic control packets to update the information about available routes.

DSR-DYNAMIC SOURCE ROUTING PROTOCOL

The Distance Source Routing (DSR) protocol is another reactive protocol; it also used to discover multiple routes to a destination node in a single discovery cycle process. If an active route fails, the source node can selects an alternative cached route. The DSR protocol is designed especially for ad hoc networks of up to two hundred nodes, as well as for mobile networks with a small diameter of 4–10 hops [15]. In the DSR protocol, the complete sequence of hops between the source and the destination is carried in each data packets send (source routing). The DSR protocol also uses RREQ and RREP messages to discover new routes. The source node that requires a route to the destination node, broadcast an RREQ message to all nodes within its transmission range. Intermediate nodes append their address to the RREQ messages and circulate it. This procedure is repeated until the RREQ message reaches to the destination node. At this time, the node responds to the initiator of the discovery process with an RREP message that includes the whole route from source to destination. The source node may be find multiple routes to the destination because it adds the new routes to its cache at each time an RREP message is received.

Along with, each implementation of the DSR protocol ‘‘may choose any appropriate strategy and algorithm for searching its route cache and selecting the best route from among those establish’’. To maintain a route when using the DSR protocol, each node that transmits a data packet must confirm that it has been correctly delivered to the next hop. This confirmation can be either a simple acknowledgement (ACK) provided by the link-layer, a passive one or one generated by a DSR-specific software. However, if the MAC protocol provides a feedback that packets have been correctly delivered, no other type of confirmation is necessary.

The DSR protocols have been maintenance a buffer, where the packets that are waiting for next-hop confirmation are stored. If the confirmation is not received after a certain number of retransmission attempt, all packets in the maintenance buffer awaiting the unreachable next hop are removed. The node that detects the broken link then generates an RERR message

once got a RERR message, sends it to the source node of the removed packet. If the nodes have another route to the destination of that removed packet, this node will replace the original source route in the packet with this route from its route cache (packet salvaging) as soon as the RERR message is sent. Then, this node forwards the packet to the next-hop, representing the alternative route. Each packet can only be salvaged a certain maximum number of times, otherwise the process repeated indefinitely. When the source node receives an RERR message, the broken links are removed from its cache and, if there is another route to the same destination, it will be used. However, if the broken route was the only path to that destination, the originator must start a new cycle process of discovery.

AODV-AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The Ad hoc On Demand Distance Vector (AODV) protocol is a distance-vector routing protocol that use a sequence numbers for to avoid the emblematic problem of distance vector protocols, known as count to infinity. To discovers a routes, the AODV protocol implements a mechanisms known as expanding ring search method. If a node have a packets to send and a route to the destination of the packet is unknown, it sends Route Request (RREQ) message. The first RREQ message is sent with a value of the Time To Live (TTL) field equivalent to one. If a time out occurs after sending an RREQ, the node broadcast another RREQ message with an increased value for the TTL field in the header. When a node receives an RREQ message, both the route to the previous hop and that to the originator of the message, are either created or updated.

The routes are updated if the sequence number of the RREQ is higher than a previous value or if the sequence number is to the same, but the new routes have a fewer hops. If the node is the destination itself or if it does know a new route to the destination node, it sends a Route Reply (RREP) message back to the source node. The nodes that receive the RREP message to create forwarding route by adding or updating the routes to the previous hop and to the destination. In the AODV protocol, there are two mechanisms for route maintenance. The first extends the route lifetime every time a packets are successfully forwarded. The second mechanism makes a node to maintain information of its active next-hop nodes, either by using link-layer notification or by listening to the channel to determine the transmission attempt from the next hops, a technique called passive acknowledgement.

If a transmission effort is not detected during the specific intervals, its connectivity is determined by receiving packets (even a HELLO message, if enabled) from the next hop, by sending an RREQ message to the next hop, or by sending an ICMP echo request to the next hop [15]. If the next-hop link could not be detected, the nodes assume that the link has been interrupted and it generates a Route Error (RERR) messages. Nevertheless, if the destination node is no further than a convinced number of hops, the node to detect the broken link attempt to repair the route locally by sending an RREQ message. If this a new route discovery process fails, the node transmits the RERR message which can either be broadcasted or iteratively unicasted to the neighbor nodes that have been originally forwarding packets on the broken route.

An RERR message can also be sent when a node get a data packet destined to a node to which it does not have an active route. When the source node receives an RERR message, a new process of route discovery will be initiated.

Table 1. Comparison of Routing Protocol Parameters.

PARAMETER	AODV	DSR	OLSR	DYMO
Routing scheme	On-demand	On-demand	Table driven	On-demand
Routing Approach	Flat	Flat	Mostly flat	Flat
Route maintenance	Route table	Route cache	Route table	Route table
Distributed	Yes	Yes	Yes	Yes

DYMO-DYNAMIC MANET ON-DEMAND ROUTING PROTOCOL

The Dynamic MANET On-Demand Routing (DYMO) protocol is a revised version of AODV protocol, also known as AODVv2. The DYMO protocol adds some of the features of the DSR to that of AODV. It is the ‘‘best suited for relatively bare traffic scenarios where any particular router forwards packets to only a small percentage of AODVv2 routers in the networks’’. The defaulting metric of the DYMO protocol is hop count, but route selection has been also based on other metrics, such as delay and energy.

In order to discover a new routes, the originator multicasts an RREQ message. The format of the RREQ and RREP messages is defined in RFC 5444; it allows the enclosure of multiple routing protocols message in a single packet. With this message format, intermediate nodes that receive either an RREP message or an RREQ message append this route from itself to the originator of the packet. This feature is called path accumulation function and it allows each node receiving an RREP message or RREQ message to update its own routing table with the information from other intermediate nodes, thus eliminates certain route discovery attempts since this information will already be available. The routes of the DYMO protocol also have a sequence number and the criterion for updating them is the same as that of the AODV protocol. Upon receiving an RREQ message, the destination node sends an RREP message in the way of the source node.

The DYMO protocol provides route maintenance similar to that of the AODV protocol. RERR messages include a list of unreachable nodes with the sequence number of the corresponding routes, and the RERR messages inform upstream nodes about the routes that are no longer available. Nodes that receive RERR messages use that information to invalidate reported routes.

OLSR- OPTIMIZED LINK STATE ROUTING PROTOCOL

Optimized Link State Routing (OLSR) is a proactive routing protocol designed essentially to reduce message overhead produced by conventional link-state protocols. In the OLSR protocol, route discovery and route maintenance are not different procedures. The routing table is updated all the time by the reception of periodical control messages of the types HELLO and TC messages. The OLSR protocol ‘‘does not generate extra traffic in response to link failures and additions’’. The routing table is re-calculated locally each time

there is a change, either in the neighbor set or in the network topology. According to, this protocol is suitable for ‘‘large and dense networks, as the technique of Multipoint Relays (MPRs) works well in this context’’ [15]. Instead of flooding the whole network with routing information, in the OLSR protocol each node selects a set of nodes, located in its 1-hop neighborhood, which will be the MPRs of that node. The neighbors of a node that do not belong to the MPR set receive broadcast packets but do not retransmit them. A source node transmitting a broadcast packet and its selected MPR set. Neighbor detection in the OLSR protocol is a fundamental task. In order to perform it, each node periodically broadcasts HELLO messages to all its immediate neighbors informing them of its link status. In this way, HELLO messages allow each node to identify its neighbors up to two hops away. These messages are received by all one-hop neighbors, but they are not necessarily forwarded.

The other type of control packets, Topology Control (TC) messages, which are broadcasted at regular intervals by every MPR, and contain the list of network nodes that have selected that MPR as a relay node. Each TC message is broadcasted through the whole network by the MPRs, and will allow each node to construct its own routing table. In the OLSR protocol, a route between two hosts is essentially a sequence of hops through the MPRs between source and destination nodes [15].

IV. CONCLUSION

We have to reviewed several routing protocols in clustering methodology, which helps to improve the performance of clustered ad hoc networks in a hierarchical manner. With this survey we see that some clustering algorithms and mainly some using routing protocols such as AODV, DSR, OLSR and DYMO. In these protocols, to compare these performances, AODV supported 50% to 60% of mobility factors. So AODV routing protocol helps to improve the efficiency of the clustered ad hoc networks.

References

[1] Ameer Ahmed Abasi, Mohamed Younnis, 21 June 2007, ‘A survey on clustering for wireless sensor networks’, Elsevier.

[2] Basu P, Khan N, Little T D C, Apr. 2001, ‘A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks’, in proceedings of IEEE ICDCSW, pp. 413-18.

[3] Chakrabarti, S, Mishra A, (2001), ‘QoS issues in ad hoc wireless networks’, IEEE Commun. Magazine. 39(2): 142-148.

[4] ‘Clustering with evolution strategies’, Pattern Recognit., vol. 27, no. 2, pp. 321-329, 1994.

[5] Coskun Cetinkaya, Vikram Kanodia, Edward W, (March 2001). ‘Scalable Services via Egress Admission control’, IEEE transaction multimedia, Vol. 3, No.1.

[6] Xuxun L, (2012). ‘A survey of clustering routing protocols in wireless sensor network’, IEEE transaction on Computer Networks.

[7] Gwo-Jong Yu, Chih-Yung Chang, (2007), 'An efficient cluster-based multi-channel management protocol for wireless ad-hoc networks', Elsevier.

[8] Amin Azari, Jalil S, Farshad Lahouti, 9 Febrauary 2015, 'Performance analysis of ad-hoc routing in heterogenous clustered multi-hop wireless networks', Elsevier.

[9] Frodigh, M., Jhansson, P, Larsson P, (2000). 'Wireless ad hoc networking: The art of networking without a network', Ericsson Rev. 4: 248-263.

[10] Ira Nath, Soumitra Das, December 2014, 'Mobility Based Clustering Algorithm for Ad Hoc Network: MBCA', International Journal, Volume 4.

[11] Javad Akbari Torkestani, Mohammad Reza Meybodi, 28 January 2011, 'A mobility-based cluster formation algorithm for wireless Mobile Ad-Hoc Networks', Springer.

[12] Jorg Habetha, Jens Wiegert, 17 October 2002. 'Analytical and simulative performance evaluation of cluster based multi-hop ad hoc networks', Elsevier.

[13] Kumarwadu P, Dechene D J, (2008). 'Algorithm for node clustering in wireless sensor networks: A survey', IEEE, 2008.

[14] Lajos Hanzo, Rahim Tafazolli, (2009). 'Admission Control Schemes For 802.11-Based Multi-Hop Mobile Ad Hoc Networks: A Survey', IEEE Communications Surveys & Tutorial, Vol. 11, No. 4.

[15] Mohammad Shokouhifa, Ali Jalali, (2014). 'A new evolutionary based application specific routing protocol for clustered wireless sensor networks', AEUE - International Journal of Electronics and Communications.

[16] Papadimitratos P, Haas Z.J., (2002). 'Secure routing for mobile ad hoc networks', In SCS Communication Networks and Distributed Systems Modeling and Simulation Conf. (CNDS 2002), San Antonio, TX.

[17] Ratish Agarwal, Mahesh motwani, (2009). 'Survey of clustering algorithm for MANET', International Journal on Computer science and Engineering, Vol. 1(2).

[18] Stephen L, Chiu, (1994). 'Fuzzy model identification based cluster estimation', Journal of Intelligent and fuzzy systems, Vol. 2, 267-278.

[19] Salamanca.P, Peña N.M., Da Fonseca, May 2013, 'A Distributed Envelope-Based Admission Control For multi-hop IEEE 802.11 Ad-hoc Networks', IEEE Latin America Transactions, Vol. 11, No. 3.

[20] Javad Akbri Torkestani, Mohammad Reza Meybodi, 28 January 2011. 'A mobility based cluster formation algorithm for wireless Mobile ad-hoc networks', Springer.

[21] Young-jun oh, Kang-whan Lee, 3 April 2015, 'A Clustering Algorithm Based on Mobility Properties in Mobile Ad-hoc Networks', International Journal of Distributed Sensor Networks, Vol. 2015.

(Received 16 March 2016; accepted 30 March 2016)

AUTHORS BIOGRAPHY

T. Parameswaran has received his B.E degree in Electronics and Communication Engineering from Velalar College of Engineering and Technology, Erode, and M.E degree in Software Engineering from College of Engineering Guindy, Anna University Chennai in 2005 and 2008 respectively. He is currently pursuing his Ph.D Anna University Chennai. He is currently working as Teaching Fellow in the Department of Computer Science and Engineering, Anna University Regional Campus, Coimbatore, Tamil Nadu, India.

C. Palanisamy has received his B.E degree in Electronics and Communication Engineering from University of Madras, Chennai and M.E degree (Gold Medalist) in Communication Systems from Thiagarajar College of Engineering, Madurai, and Madurai Kamaraj University in 1998 and 2000 respectively. He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 15 years of academic and research experience and currently he holds the post of Professor and Head of the Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India. He has published more than 40 research papers in various journals and conferences. He has organized more than 15 workshops and holds 2 funded projects. He is a lifetime member of ISTE. He Won Best M.E Thesis Award at Thiagarajar College of Engineering, Madurai and best paper award titled, "A Neural Network Based Classification Model Using Fourier and Wavelet Features," Proceedings of the 2nd Int. Conf. on Cognition and Recognition 2008, (ICCR 2008), Organized by P.E.S. College of Engineering, Mandaya, Karnataka, India, pp. 664-670, 2008. His research interests include Data mining, image processing, and mobile networks.

P. Bhagya davi received the Bachelor Degree in Information Technology from Anna University of Technology; Thiruchirappalli in 2014. She is currently pursuing her Master Degree in Software Engineering from Anna University Regional Campus, Coimbatore, Tamil Nadu, India. Her area of interest is networking.