RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of MANET Routing Protocols and Cluster Head Selection Technique in MANET

Mr. Pratik Gite[1], Dr. Sanjay Thakur[2]
[1]Pacific Academy of Higher Education and Research University, Udaipur, (R.J.), India
[2]Pacific Academy of Higher Education and Research University, Udaipur, (R.J.), India

Abstract
Mobile Ad-hoc Network is a kind of wireless network. It is a backbone of new generation advanced communication technology. MANET is an ideal applicant for rescue and emergency situation due to its independence of connected devices of fixed wires. This paper represents a work on trust based system in MANET cluster that can be used to improve the performance of the network even in the existence of not trusted nodes. In the cluster architecture, cluster head and gateway nodes form a communication for routing among neighbouring clusters. But selection of cluster head is the important problem in dynamic Ad-hoc network because cluster head work as coordinator in clustered architecture. In this work, some values have used correspond to the threshold values of forward packet and dropped packet of each node within the network cluster. These values have been used dynamically updated every time and the node is selected as cluster head. In this technique of selecting the node as cluster head, the node which has maximum trusted value is elected as cluster head and this information is updated in every node's trusted table. After implementation of our desired work, the proposed Dynamic Trust Evaluation of Cluster Head (DTE-CH) technique is analysed with traditional routing protocols and traditional clustering technique viz. Highest Degree Algorithm. The simulation is done by using network simulator software on the basis of different performance metrics throughput, packet delivery ratio, routing overhead, packet drop, average end to end delay and remain energy. Simulation result presents that proposed DTE-CH technique improves the performance of network as compare to most suitable existing AODV MANET protocol based technique as well as traditional highest degree clustering technique.
Keywords— MANET, Routing Protocols, Highest Degree Clustering Algorithm, Proposed DTE-CH Algorithm

I. INTRODUCTION

Mobile Ad-hoc Network is a rapid configurable network. In addition to that the mobility is an essential property of the network [7]. Due to this reason, the topology is dynamically created whenever required [8]. Thus there are mainly two kinds of data delivery approaches utilized for organization of network. First using the routing protocols like DSDV, AODV and DSR. Secondly, for efficiency clustering approaches are used. This paper is concern about the brief study of MANET routing protocols and traditional clustering techniques. There are basically two objectives of this paper. First is to analyse the MANET routing protocols to select efficient protocol for small network as well as large network. Second is to evaluate the performance of network under traditional highest degree clustering algorithm, Proposed DTE-CH algorithm and traditional MANET protocol.

II. DSDV, AODV AND DSR ROUTING PROTOCOLS

DSDV: - Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. The improvement made to the Bellman-Ford algorithm includes freedom from loops in routing tables by using sequence numbers. It was developed by C. Perkins and P. Bhagwat in 1994. The DSDV protocol can be used in Mobile Ad-hoc Network environments by assuming that each participating node acts as a router. Each node must maintain a table that consists of all the possible destinations. In this routing protocol, an entry of the table contains the address identifier of a destination, the shortest known distance metric to that destination measured in hop counts and the address identifier of the node that is the first hop on the shortest path to the destination. Each mobile node in the system maintains a routing table in which all the possible destinations and the number of hops to them in the network are recorded. A sequence number is also associated with each route/path to the destination. The route labelled with the highest sequence number is always used. This also helps in identifying the stale routes from the new ones, thereby avoiding the formation of loops. Also, to minimize the traffic generated, there are two types of packets in the system. One is known as "full dump", which is a packet that carries all the information about a change. However, at the time of occasional movement, another type of packet called "incremental" will be used, which will carry just the changes, thereby, increasing the overall efficiency of the system. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks [4].

DYNAMIC SOURCE ROUTING: Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks and is based on a method known as source routing. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. Except that each intermediate node that broadcasts a route request packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply message that includes the list of addresses received in the route request and transmits it back along this path to the source. Route maintenance in DSR is accomplished through the confirmations that nodes generate when they can verify that the next node successfully received a packet. These confirmations can be link-layer acknowledgements, passive acknowledgements or network-layer acknowledgements specified by the DSR protocol. However, it uses source routing instead of relying on the routing table at each intermediate device. When a node is not able to verify the successful reception of a packet it tries to retransmit it. When a finite number of retransmissions fail, the node generates a route error message that specifies the problematic link, transmitting it to the source node. When a node requires a route to a destination, which it doesn't have in its route cache, it broadcasts a Route Request (RREQ) message, which is flooded throughout the network. The first RREQ message is a broadcast query on neighbours without flooding. Each RREQ packet is uniquely identified by the initiator's address and the request id. A node processes a route request packet only if it has not already seen the packet and its address is not present in the route record of the packet [5]. This minimizes the number of route requests propagated in the network. RREQ is replied by the destination node or an intermediate node, which knows the route, using the Route Reply (RREP) message. The return route for the RREP message may be one of the routes that exist in the route cache (if it exists) or a list reversal of the nodes in the RREQ packet if symmetrical routing is supported. In other cases the node may initiate it owns route discovery mechanism and piggyback the RREP packet onto it. Thus the route may be considered unidirectional or bidirectional. DSR doesn't enforce any use of periodic messages from the mobile hosts for maintenance of routes. Instead it uses two types of packets for route maintenance: Route Error (RERR) packets and ACKs. Whenever a node encounters fatal transmission errors so that the route becomes invalid, the source receives a RERR message. ACK packets are used to verify the correct operation of the route links. This also serves as a passive acknowledgement for the mobile node. DSR enables multiple routes to be learnt for a particular destination. DSR does not require any periodic update messages, thus avoiding wastage of bandwidth [6].

AODV: AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV.

Basic Mechanisms

When a node S needs a route to some destination D, it broad-casts a ROUTE REQUEST message to its neighbours, including the last known sequence number for that destination. The ROUTE REQUEST is flooded in a controlled manner through the network until it reaches a node that has a route to the destination. Each node that forwards the ROUTE REQUEST creates a reverse route for itself back to node S. When the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPLY that contains the number of hops necessary to reach D and the sequence number for D most recently seen by the node generating the REPLY. Each node that participates in forwarding is REPLY back toward the originator of the ROUTE REQUEST (node S), creates a forward route to D. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing. The basic functionality of AODV is shown in figure 1.

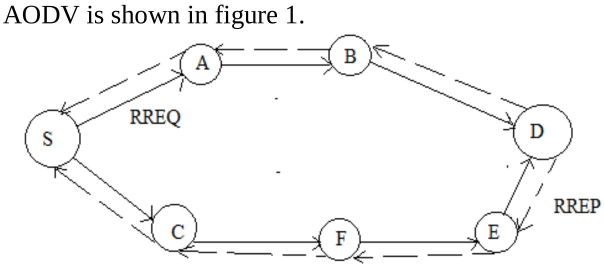

Figure 1 AODV Routing

In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbour is taken as an indication that the link to the neighbour in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbours [10]. When a link goes down, any upstream node that has recently forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPLY containing an infinite metric for that destination. Upon receipt of such a ROUTE REPLY, a node must acquire a new route to the destination using Route Discovery as described above [10].

III. CLUSTERING TECHNIQUES

Wherever, Mobile Ad-hoc Networks (MANETs) are created randomly by a set of mobile nodes which cover others with the help of their transmission range. Mobile Ad-hoc Network does not depend on fixed infrastructures and they operate without any centralized administration [11]. Mobile nodes are using dynamic topologies as nodes are capable of moving aggressively [12]. Routing protocols act as the required steps in MANETs and assist communication outside the physical wireless coverage of the nodes. To provide connectivity, every node needs cooperation from other nodes to distribute packets to their destination by performing as a router [13]. These protocols could function in either a normal or hierarchical network environment [13]. In the normal architecture, all nodes contribute in the routing procedure. In the hierarchical design nodes are separated into a number of clusters each of which is managed by a cluster-head that manage decisions for cluster members. In this environment only cluster heads and gateway nodes, intermediate nodes between two cluster-heads can participate in the routing [14]. Figure 2 shows the inter cluster and intra cluster communication between nodes.

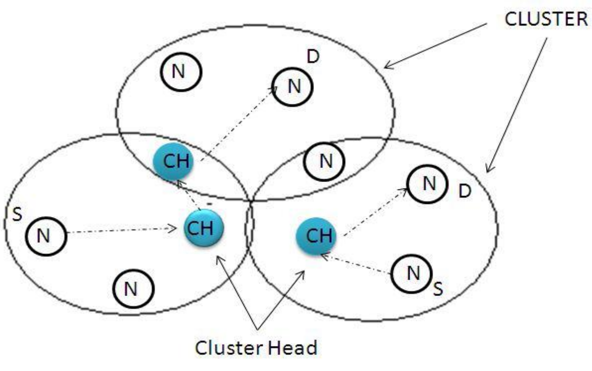

Figure 2 Inter cluster and Intra Cluster Communication between Nodes

Established MANET routing protocols assume that all nodes in the network have no trust among each other. This may cause the network exposed to malicious attacks. The selfish and malicious nodes are threat to network in order to save their own batteries they do not transmit packets from other nodes as instructed by the protocol [14]. Since the communication reliability of a node exclusively depends on a proper option of the path used to make the destination, it is significantly important for a host to know the reliability of the nodes forming the route [15].

IV. VARIOUS CLUSTERING TECHNIQUES

In this section, various kinds of Ad-hoc Network clustering approaches are discussed in detail with their appropriate domain of classification [23]:

A. Connectivity Based Clustering

In connectivity based clustering approach, the connectivity between nodes is the essential property for cluster-head formation. The relevant approaches of such technique are discussed in this section.

1. K-hop Connectivity ID Clustering Algorithm:

It combines two clustering algorithms namely Lowest- ID and Highest-degree heuristics. At the initiation, node starts a flooding process in which a clustering request is sent to all nodes. If using only a lower ID clusters then more clusters unnecessary generated thus result is a set of cluster-heads increases. Thus, result is a set of cluster-head increases. On the other hand using only node connectivity causes numerous of evaluation between nodes. So, by combining both can limit on number of clusters. The node having highest connectivity is selected as the cluster-head, when number of hops k=1, connectivity is same as node degree. K-CONID generalizes connectivity for a k-hop neighbour-hood and if degree of connectivity of two nodes is same then priority node is selected with lowest ID. So, every node maintains two parameters. These parameters are degree of connectivity and lowest ID [23].

2. Highest Connectivity Clustering Algorithm:

Each node broadcasts its id to nodes that are within its transmission range. The node with maximum number of neighbours is chosen as a cluster-head. Since no cluster-heads are directly linked, only one cluster-head is allowed per cluster. Any two nodes in a cluster are at most two hops away since the cluster-head is directly linked to each of its neighbours in cluster. The systems also have some limitations which are given in following manner [23]:

- **i)** The system has a low rate of cluster-head change but the throughput is low. Typically, each cluster is assigned some resources which is shared among the members of that cluster. (CH) are shared between all its neighbours So, CH becomes a bottleneck.
- **ii)** As well as the maximum number of nodes in a Cluster is unlimited.

iii) The re-affiliation count of nodes is high due to node movements and as a result, the highest-degree node may not be re-elected to be a cluster-head even if it loose one neighbour.

3. Adaptive Cluster Load Balance Method:

In HCC clustering scheme, one cluster head can be exhausted when it serves too many mobile hosts. It is not desirable and CH becomes a bottleneck. So a new approach is given. In hello message format, there is an "Option" is available. If a sender node is a cluster head, it will set the number of its dominated member nodes as "Option" value. When a sender node is not a cluster head or it is undecided, "Option" will be reset to 0. When a CH's Hello message shows its dominated nodes' number exceeds a threshold, no new node will participate in this cluster. As a result, this can eliminate the CH bottleneck phenomenon and optimize the cluster structure. This algorithm can get load balance between various clusters. Thus, resource consumption and information transmission is distributed to all clusters instead of few clusters [23].

B. MOBILITY BASED CLUSTERING:

1. Mobility Based Metric for Clustering:

It proposes the partitions of an Ad-hoc Network into D-hop clusters based on mobility metric. The clusters are formed in such a way mobile nodes with low speed relative to their neighbours become cluster-heads. The aggregate mobility metric is computed over a small time by calculating the difference of relative mobility between a node and all its neighbours. The only dissimilarity between Lowest-ID and MOBIC is that it uses mobility metric for cluster formation instead of ID information. In this algorithm, received power of transmissions of two successive Hello message is measured by each node from every neighbour. First, the pair wise relative mobility metrics is calculated and then aggregate relative mobility metric is computed before transmitting the next packet. In Hello message, every node broadcasts its own mobility metric to its 1-hop neighbor and it is stored in the neighbour table with a timeout period. In such way, every node receives the aggregate mobility from its neighbouring nodes and compares its own mobility with its neighbors. The node having the lowest mobility value amongst all its neighbours is selected as cluster-head. The conditions are [23]:

i) If a node with Cluster Member status having low mobility into the range of another Cluster Head node which having higher mobility, then re-clustering is not done.

ii) If two nodes having status Cluster Head move into each other's range, re-clustering is deferred for Cluster Contention Interval (CCI) to permit for incidental contacts between passing nodes.

iii) If the nodes are in transmission range of each other even after the Cluster Contention Interval timer has expired, re-clustering is triggered and the node with the lower mobility metric is selected as cluster head.

iv) In case of particular scenarios, where the relative mobility between nodes does not differ drastically, the mobility metric gives better results [23].

C. COMBINED WEIGHTED BASED CLUSTERING

In such kind of clustering algorithm a normalized weight is calculated for creating a cluster [23].

1. Weighted clustering algorithm (WCA):

The WCA is based on the use of a merged weight metric. For cluster-head election the metrics used are the number of neighbours, distance with all neighbours, mobility and cumulative time for which the node acts as the cluster-head. By rebroadcasting each node knows the weight values of all other nodes and information of other cluster-heads in the system. So, there is high overhead induced by WCA. The drawback of WCA is, if a node moves into an area it is not covered by any cluster-head then the cluster set-up procedure is invoked again which causes re-affiliations. A Hello message comprises its ID and position. Each node builds its neighbour list based on the Hello messages received. Each node computes its weight value by following algorithm.

a) Find the set of neighbours of each node v called N(v). (e.g. if the distance between v and v' is less than the transmission range of v then v' is neighbour of v). Set dv, the degree of v.

b) Calculate the degree-difference for each node, where δ pre-defined threshold is means the number of nodes that a cluster-head can handle ideally.

$$\Delta_v = |d_v - \delta|$$

c) For every node, calculate the sum of the distances Dv with all its neighbours. Then compute the running average of the speed for every node until current time T. This gives a measure of mobility Mv where (Xt, Yt) defines the position of the node v at instant.

$$M_v = \frac{1}{T}\sum_{t=1}^{t}\sqrt{(X_t - X_{t-1})^2(Y_t - Y_{t-1})^2}$$

Compute the cumulative time Pv during which a node v acts as cluster-head. Pv indicates how much battery power has been consumed, which is assumed more for a cluster-head than an ordinary node.

d) Calculate the combined Weight (Wv) for each node v where

$$W_v = W_1 * \Delta_v + W_2 * D_v + W_3 * M_v + W_4 * P_v$$

Where the node with the smallest Wv is elected as cluster-head and then all ordinary nodes of the selected cluster-head are not allowed to participate in the election process

e) Repeat steps 2 to 5 for the remaining nodes which are not yet selected as a cluster-head or assigned to a cluster.

2. An Efficient Weighted Distributed Clustering (CBMD):

It uses different weight function which takes into consideration the parameters: connectivity (C), residual battery power (B), average mobility (M), and distance (D) of the nodes to choose locally optimal cluster-heads. Advantages of these clustering algorithms are load balancing between the clusters is achieved and less number of clusters formed by specifying the maximum and minimum number of nodes that a cluster-head can ideally handle. Furthermore, each mobile node starts to measure its weight after n (small integer in order to minimize the memory requirement) successive HELLO messages, where the result specifies the accurate value for the mobility and battery power. This algorithm is used to elect optimal cluster-heads and divide optimal number of clusters without degrading the whole network performance, to satisfy the load balancing between clusters, to maximize the cluster stability and to reduce the communication overhead and minimizing the explicit control messages caused by cluster maintenance [23].

3. Distributed Weighted Clustering Algorithm:

It works same as WCA except that power management and distributed cluster set up is done by localizing configuration and reconfiguration of clusters. The consumed battery power is a better determine than the cumulative time during which the node acts as a cluster-head that is used in WCA because it reflects the actual amount of power usage. If there is inadequate battery power then lifetime of topology can be enhanced by switching the role of the cluster-head to an ordinary node. Two situations can invoke the cluster maintenance phase, when there is node movement outside of its cluster boundary and when there is excessive battery consumption at the cluster-head. When an ordinary node moves outside of its cluster boundary, it is needed to find a new cluster-head to affiliate with. If it finds a new cluster-head, it hands over to the new one cluster. If not, it declares itself as a cluster-head. Each cluster-head modified the amount of consumed battery power when it sends and receives packets. If the amount of consumed battery power becomes more than a pre-defined threshold value then the cluster-head resigns and becomes an ordinary node. This algorithm offers better performance than WCA in terms of the number of re-affiliations, end-to-end throughput, overheads during the primary clustering set up phase, and the lifespan of nodes [23].

V. PERFORMANCE ANALYSIS OF DSDV, AODV AND DSR

To select best protocols for further analysis of MANET environment with traditional clustering techniques and newly proposed clustering technique, the simulation based analysis of MANET routing protocols is done by using network simulator software on the basis of different performance metrics. The results are discussed bellow.

THROUGHPUT: It is the amount of data per unit time that is delivered from one node to another via a communication link [4]. The throughput of the network provides the information how the network efficiently provides the services to their clients. That is measured for finding the available bandwidth consumption in terms of MBPS or KBPS. Efficient routing protocols must have greater throughput.

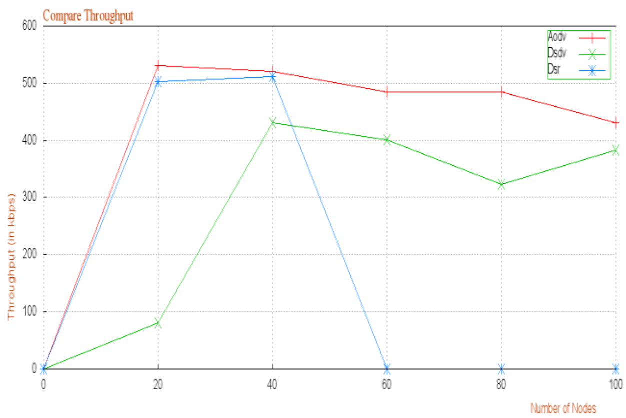

Figure 3 Throughput with Number of Varying of Nodes

The given figure 3 shows the throughput comparison of DSDV, DSR and AODV routing protocols. In order to show the performance of the AODV routing protocol the red line is used, for demonstration of DSDV green line is used and for DSR routing protocol blue line is used. In this figure the X axis represents the number of nodes in the network and the Y axis shows the throughput of the network. According to the obtained results the AODV routing protocol provides much consistent and constant bit rate as compared to DSDV and DSR routing protocol. On the other hand the throughput of DSDV and DSR routing protocol is much affected as the number of nodes in the network increases and throughput of the

AODV is not so much affected as the number of node increases and decreases in the network.

PACKET DELIVERY RATIO (PDR): The packet delivery ratio is expressed as the percentage of number of received packets by destination node to number of packets sent by all the source nodes within the period of simulation time [5]. It is the essential performance metrics of routing protocols. Higher the value of packet delivery ratio gives the better results. The Packet Delivery Ratio comparison of the DSDV, AODV and DSR routing protocols are demonstrated using figure 4 with increasing number of nodes.

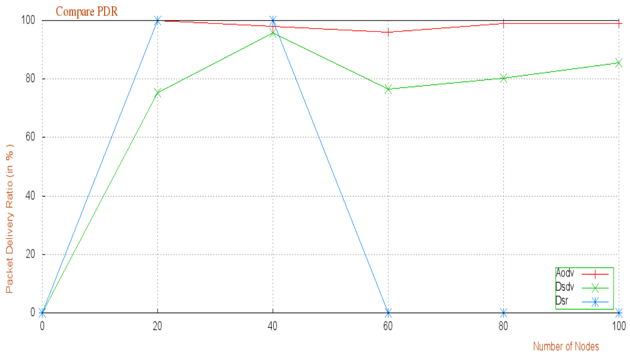

Figure 4 PDR with Number of Varying of Nodes

In order to represent the performance of routing protocols, the X axis contains number of nodes and the corresponding percentages of delivered packets are given using Y axis. According to the obtained results the performance of DSR and AODV routing protocol in terms of Packet Delivery Ratio is much adoptable as compare to the DSDV for 20-nodes and 40-nodes scenario because in most of the experiments both the protocol delivers similar amount of data. But as the number node increases in the network AODV perform better among the three protocols and DSR does not provide very much efficiency as compare to both in high number of nodes.

ROUTING OVERHEADS: Routing overheads is the number of control packets generated by each routing protocol during simulation. It is the internal measure or efficiency of any routing protocols. Two different routing protocols can use different amounts of overheads depending on their internal efficiency. If control and data traffic share the same channel and channel capacity is limited then excessive control traffic often impacts data routing performance (throughput). If more control packets are sent by the routing agents, then delay in the network will also increase [2]. The routing overhead comparison of the DSDV, AODV and DSR routing protocols with the increasing number of nodes are given using figure 5. In this figure, the amount of overhead is represented using Y axis and the number of nodes shown using X axis.

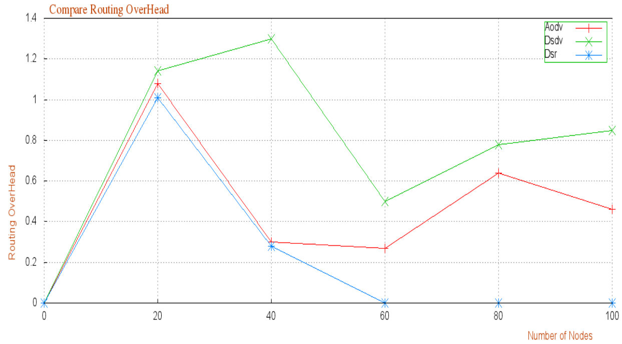

Figure 5 Overheads with Number of Varying Nodes

According to the obtained results the performance of DSR routing protocol is better than DSDV and AODV routing protocols in terms of routing overhead for 20, 40, 60, 80 and 100 nodes scenario. Therefore, DSR is more adoptable for this performance metrics in Mobile Ad-hoc Network Routing. Basically DSDV sends periodically routing information to one node to another in throughout the network as maintain consistent network view and AODV also needs to send some more routing packets during the transmission and retransmissions of data as compare to the DSR routing protocols. So, DSDV and AODV having more routing overheads as compare to the AODV routing protocol.

AVERAGE END TO END DELAY: The total amount of time required to deliver data from source to destination is given using end to end delay. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges [4]. Here the estimated delays of networks are measured in terms of milliseconds and simulated using Y axis as given figure 6.

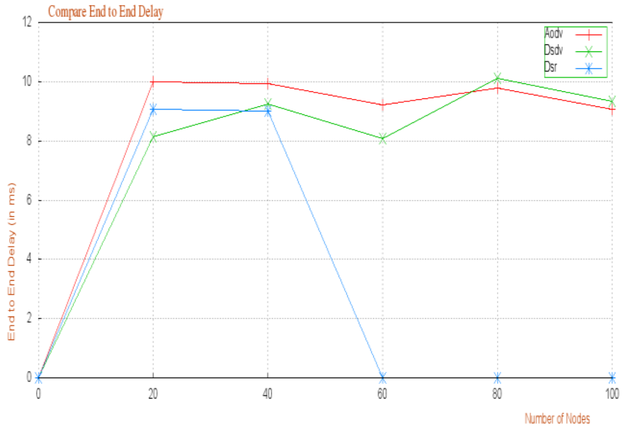

Figure 6 Average End to End Delays with Number of Varying Nodes

Additionally X axis shows the number of nodes in network. According to the obtained simulation results, the average end to end delay of DSDV, AODV and DSR routing protocol is also increases and decreases as the number of nodes increases and decreases in the network. In the analysed scenario, it is found that, the average end to end delay of AODV is maximum for 20, 40 and 60 nodes scenario and that of DSR is moderate for 20 nodes and minimum for 40, 60, 80 and 100 nodes scenario. But in case of 80 and 100-nodes average end to end delay of DSDV is maximum and that of AODV is minimum. Basically, DSDV sends periodic data exchange between the neighbour nodes thus that increases the additional packets in network and in AODV the delay is also produces due to updating of routing tables information in case of new route initiation in the network.

PACKET DROP: The amount of packet failed during the transmission of data is known as the packet drop [5]. A packet is dropped in two cases: the buffer is full when the packet needs to buffer and the time that packet has been buffer exceeds the limit. The figure 7 shows the packet drop of the network where the comparative results among AODV, DSDV and DSR routing is provided.

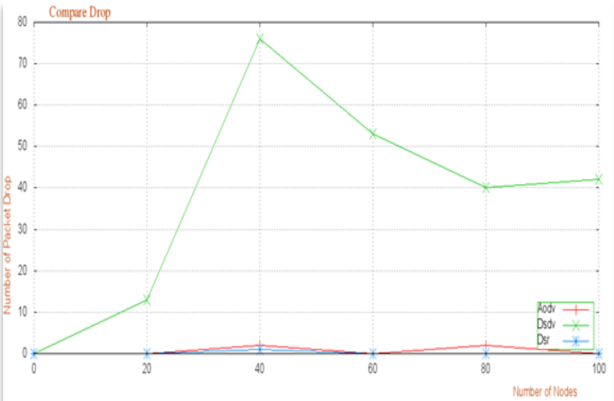

Figure 7 Packet Drop with Number of Varying Nodes

The amount of packet drops in AODV and DSR routing protocol is much similar from each other because that is indirectly proportional to packet delivery ratio. Thus if the packet delivery ratio is higher than the packet drop ratio is less and vice versa. According to the obtained results, the packet drop for DSDV routing protocol is maximum and that of AODV and DSR routing protocol is minimum and much similar for 20, 40, 60, 80 and 100 nodes scenario.

REMAIN ENERGY:

The amount of energy preserved during the active sessions of communication is known as remain energy. The Ad-hoc devices are developed with the inbuilt energy sources therefore for each event in network a fixed amount of energy is consumed from the initial energy. Figure 8 shows the amount of remain energy in different routing sessions over increasing number of varying nodes.

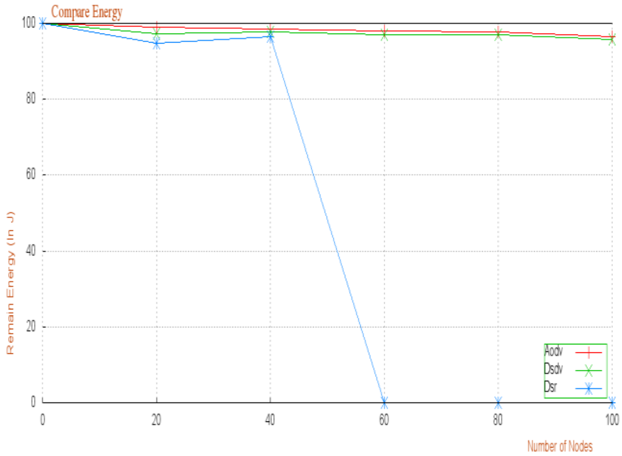

Figure 8 Remain Energy with Number of Varying of Nodes

In this figure, the percentage amount of remain energy is given on Y axis and the X axis contains the number of nodes in the network. According to the evaluated results in terms of remain energy AODV routing protocol is maximum and that of DSDV is minimum. Basically, DSR consumes more energy as compare to the DSDV and AODV routing protocol. In the analysed scenario it is found that according to the MANET property, low battery can affect the network functioning thus the DSR is not much effective for the long simulations. Additionally, the DSR is not much supportive for the large network.

Subsection Conclusion: - This sub section provides a brief study of the DSDV, AODV and DSR routing protocols theoretically and through simulation. Further, different performance issues associated with these routing protocols are discussed in detail. In this study it is analysed that, the key element of the entire network functioning depends on the routing strategy. Therefore, DSDV, AODV and DSR routing protocols are analysed in terms of throughput, packet delivery ratio, routing overhead, packet drop, average end to end delay and remain energy. In order to obtain the efficient and reliable communication for small and large networks, the performance study made among the AODV, DSDV and DSR routing protocols is done. In this comparison AODV routing protocol is found most reliable routing technique because this is much flexible to support small networks as well as large networks. In addition to that, in other performance parameters such as throughput, packet delivery ratio, remain energy, packet drop the AODV routing protocol is much efficient than the DSDV and

DSR routing protocol for varying number of nodes but the key factor is that AODV routing protocol is also energy saving technology too, because of the less control message exchanges and less periodic message exchanges. Therefore, the AODV routing is obtained as the most optimum routing protocol for the remaining experimentations.

VI. DYNAMIC LEADER SELECTION TECHNIQUE

Various researchers have been carried out detailed study on cluster based routing in MANET. Trust is one of the main aspects these are considered while developing routing protocols. Trust value of any node represents its participation and reliability in network. A node which is having very low trust among its neighbour affect the MANET services provided such as unreliable services, suddenly breakdown in services and soon. These types of nodes are always avoided by their neighbours. A node's trust value is decided by various factors. These factors include **dropped packet**, **forward packets** and **packet receive** by un-trusted nodes. Some researchers proposed various scheme to calculate and analyse the trust value of nodes. Some mechanism proposed a method in which each node is chosen as cluster head based on the influence of the trust value evaluated by the neighbours, level of a node, stability and battery level. Each node is treated as malicious node or a normal node based on its earlier behaviour. For cluster head determination, each node can propose one of its neighbours as cluster head. The objective of the proposed idea is the dynamic cluster head appointment for reliable data transmission in trusted MANET environment. In our approach, a cluster head position is changing among the nodes at a predefined interval. A node cannot acquire cluster head position for along time. Position rotation among the nodes make the cluster head trust value more reliable and secure. If a node behaves as an un-trusted nodes then it is dismissed from its position and new cluster head selection mechanism selected the most reliable and trusted node as cluster head. When a node joins MANET, then its trust value is assumed and assigned. Most of the time, this value is equal to one. For calculating, the trust value our approach maintains a table at each node is called trust table. This table is maintained by every node and must be updated at an interval in addition to their neighbour tables. At each node, trust table includes N**ode Id, Number of Packets Forwarded, Number of Packets Dropped, Number of Packets Received.** These values are calculated on the basis of nodes performance within the cluster and outside the cluster. This cluster information table is updated after an interval. Trust value of each node is calculated on the basis of trust factors. These trust factors includes some threshold values. These threshold values depend on some dynamic behaviour of nodes within the cluster.

$$Trust_{incluster} = P_f^{intotal} * \alpha^{th} + D_p^{intotal} * \beta^{th}$$

$$Trust_{outcluster} = P_f^{out} * \alpha^{th} + D_p^{out} * \beta^{th}$$

$$Trust_{clusterhead} = trust_{incluster} + trust_{outcluster}$$

Here P_f^{in} and D_p^{in} are the number of packet forwarded and dropped within the cluster and outside the cluster respectively. f_{in}, p_{in}, f_{out} and P_{out} are received packet and sent packet from the nodes of the same cluster to the nodes of same cluster or other cluster and to the same cluster or other cluster respectively. In our proposed work, we have used some threshold values α and β. These values are correspond to the threshold values of forward packets and dropped packets of each node within the cluster. These values are updated every time the node is appointed as cluster head. In the process of selecting the cluster head the node, the nodes which have maximum trusted value is elected as cluster head and this information is updated in every node's trusted table.

VII. PROPOSED DTE-CH SELECTION ALGORITHM

The entire process of the cluster head selection on the basis of new method is given using the steps.

Step1: Initialize the network with N nodes

$$N = \{n_1, n_2, \dots n_m\}$$

Step 2: For each node in network enable and initialize the trust tables

For i=1 to m

(Where m is highest value of node)

$$n_i \leftarrow initilize(trustTable)$$

End for

Step 3: For i=1 to m (For each time interval T Compute node's trust values)

$$Trust_{incluster} = P_f^{in} * \alpha^{th} + D_p^{in} * \beta^{th}$$

$$Trust_{outcluster} = P_f^{out} * \alpha^{th} + D_p^{out} * \beta^{th}$$

$$Trust_{clusterhead} = trust_{incluster} + trust_{outcluster}$$

End for

Step 4: For i=1 to m

(Exchange the trust values and compare them for cluster head selection

For each connected node)

If node trust value >neighbour trust values

Broadcast self as cluster head

End if

End for

VIII. SIMULATION RESULTS AND ANALYSIS

The simulation results of newly proposed technique, existing AODV routing protocol and highest degree algorithm are shown in the following section in the form of comparative graphs. The simulation analysis of the protocols primarily focuses on a few performance metrics. The following metrics are used in this work for the performance evaluation of traditional AODV Highest Degree Algorithm and new proposed DTE-CH algorithm.

1. THROUGHPUT

The throughput is calculated at destination node during entire simulation period. In this subsection, throughput of proposed DTE-CH algorithm, AODV routing protocol and Highest Degree Algorithm is calculated for different number of nodes. The variation of throughput with the number of nodes under AODV, Highest Degree Algorithm and proposed DTE-CH algorithm is shown in figure 9.

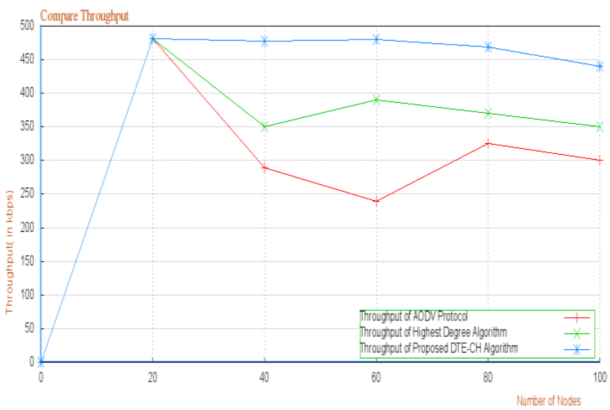

Figure 9 Throughput of AODV, Highest Degree and DTE-CH Algorithm

According to the obtained results, the throughput of the DTE-CH technique is maximum, AODV protocol is minimum and Highest Degree Algorithm is between the two. The key advantage of the proposed DTE-CH technique is that, it would work on the dynamic leader selection of cluster based approach. Thus it improves the connectivity and data delivery ratio as well as improves the network performances and bandwidth consumption for internal as well external communication scenario.

2. DATA PACKET DROP

The number of data packets that are not successfully sent to the destination. Basically, it is defined as the number of packets drop to the total number of packet generated during the simulation time. Lower the packet drop, lower would be the delay in the network.

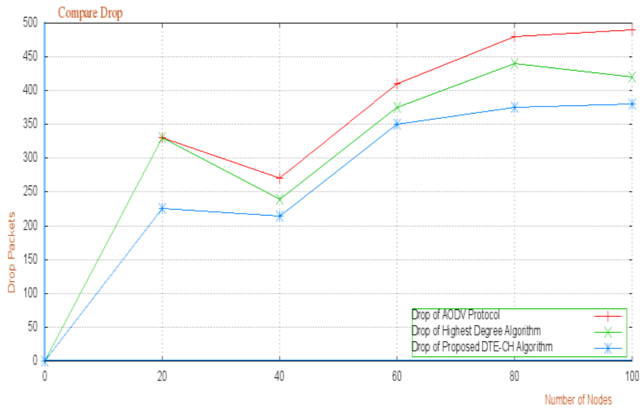

Figure 10 Drop of AODV, Highest Degree and DTE-CH Algorithm

According to the obtained results, the packet drop of existing AODV protocol is maximum, proposed DTE-CH is minimum and highest degree algorithm is between the two for number of varying nodes. As per the given results, the proposed secure clustering technique improves the connectivity as well as the throughput thus the nodes optimized for transmitting more data with more reliable environment. Thus, the performance of the network in terms of packet drop ratio is also improved as compared to the traditional AODV routing protocol and highest degree algorithm.

3. AVERAGE END TO END DELAY

Average end to end delay on network refers to the time taken for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula. E2E delay = receiving time – sending time. The comparative network performance in terms of end to end delay is given below:

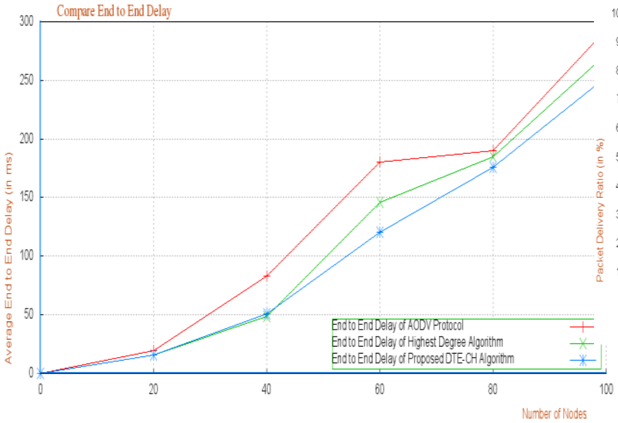

Figure 11 Delays of AODV, Highest Degree and DTE-CH Algorithm

According to the obtained results, the average end to end delay of the existing AODV protocol is maximum, proposed DTE-CH is minimum and that of highest degree is between the two. Basically the end to end delay reduces in the proposed technique because the address of the cluster head and destination nodes are known by the cluster heads thus for identifying the node location needs less time and that phenomena improves decision efficiency in terms of end to end delay in cluster oriented network as compared to the traditional way of routing.

4. ROUTING OVERHEAD

It is the total amount of control data packets generated by each routing protocols throughout the duration of simulation experiment.

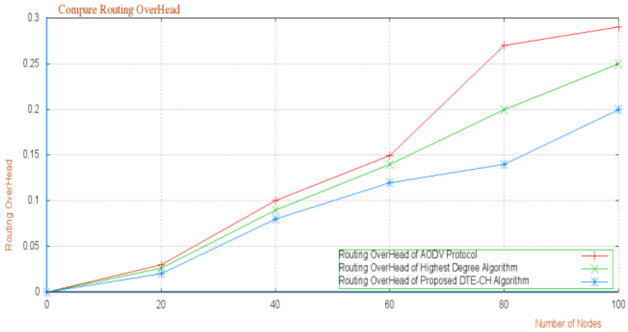

Figure 12 Overhead of AODV, Highest Degree and DTE-CH Algorithm

According to the obtained results, the routing overheads of existing AODV protocol is maximum, proposed DTE-CH is minimum and highest degree algorithm is between the two.

5. PACKET DELIVERY RATIO

It is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source node. It can be calculated in terms of percentage (%).

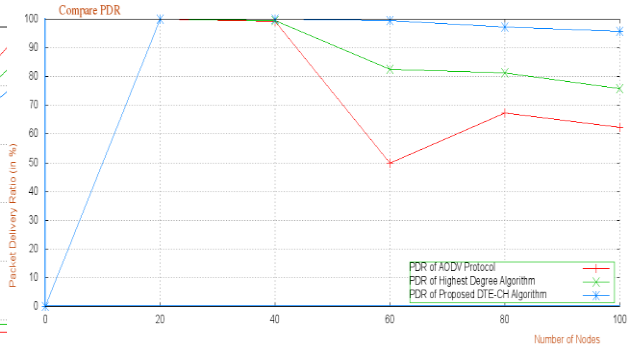

Figure 13 PDR of AODV, Highest Degree and DTE-CH Algorithm

According to the obtained results, the routing overheads of existing AODV protocol is maximum, proposed DTE-CH is minimum and highest degree algorithm is between the two for number of varying nodes.

6. REMAIN ENERGY

The mobile nodes are developed with the limited amount of energy source thus for each event in network the significant amount of energy is consumed. After completing the simulation the amount of battery power remain is known as remain energy.

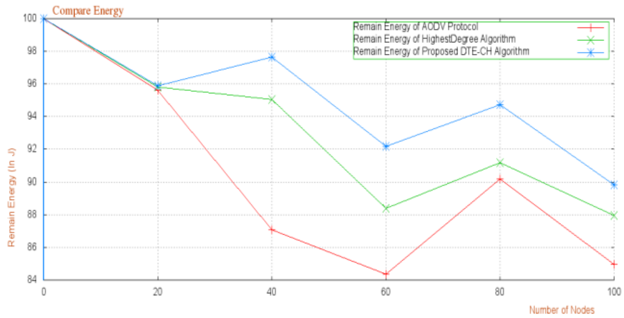

Figure 14 Energy of AODV, Highest Degree and DTE-CH Algorithm

According to the obtained results, the remaining energy of existing AODV protocol is maximum, proposed DTE-CH is minimum and highest degree algorithm is between the two.

IX. CONCLUSION AND FUTURE SCOPE

In MANET, mobile nodes are known to their changing location. Therefore, frequent location change of nodes affects the network performance. A network needs to maintain the routing information and restart all the routing process when a node changes its location. A better selection mechanism should be implanted to provide a better way to assign a node to cluster head position. In this research work, a new technique is developed that assign a node to a cluster head position after a fair selection process.

This cluster head selection process is started every time in the predefined interval or if cluster head node behaves as a malicious node. A node which has maximum trust value is elected as cluster head and updated in all nodes cluster table. A trusted node reputation value is required to be sustained and improved. A not trusted node is a threat for a network performance. So, it should be avoided and blocked by the network. According to above discussed simulation results, first performance analysis of MANET routing protocols is done and best routing protocols is selected for further experimentations with highest degree algorithm based clustering technique and proposed DTE-CH algorithm based clustering technique for finding the effectiveness of MANET performance in terms of throughput, packet delivery ratio, routing overheads, average end to end delay, packet drop and remain energy.

In the analysed scenario, it is found that the throughput of proposed DTE-CH algorithm is better than AODV routing protocol and highest degree algorithm for 20-nodes, 40-nodes, 60-nodes, 80-nodes and 100 nodes scenario. The Packet Loss of proposed DTE-CH algorithm is minimum and AODV Routing Protocol is maximum and that of highest degree algorithm is between the two for 20, 40, 60, 80 and 100-Nodes and 100-Nodes scenario. Simulation results of Average End to End Delay shows that the AODV Routing Protocol has maximum Average End to End Delay and proposed DTE-Ch has minimum delay and highest degree is between the two. Simulation results of routing overhead shows that AODV Routing Protocol has maximum routing overhead and proposed DTE-CH has minimum routing overhead and highest degree algorithm is between the two. According to above simulation results, the packet drop of AODV is maximum, proposed DTE-CH algorithm is minimum and that of highest degree algorithm is between the two for 20-nodes, 40-nodes, 60-nodes, 80-nodes and 100 nodes scenario. Simulation results of Remain Energy shows that, AODV has maximum remain energy, proposed DTE-CH algorithm has minimum remain energy and that of highest degree algorithm is between the two for 20-nodes, 40-nodes, 60-nodes, 80-nodes and 100 nodes scenario. In the analysed scenario, it is found that our proposed protocol is better in network cluster environment and provides a better approach to elect cluster head in trust environment. The given-technique is much promising for electing efficient cluster heads thus that can be extendable for the different security schemes for wireless network technology. Therefore in near future the given technique is implemented with additional network characteristics for applying the security for trusted management schemes.

REFERENCES

[1] **J. Broch, D. A. Maltz, D. B. Johnson, Y.C. Hu and J. Jetcheva,** "*A Performance Comparison of Multi-hop Wireless Ad-hoc Network Routing Protocols*", Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, PP. 85-97, ACM Press, 1998.

[2] **A. Boukerche,** "*Performance Comparison and Analysis of Ad-hoc Network Routing Algorithms*", IEEE Conference on Performance, Computing and Communication, PP.171-178, April 2001.

[3] **D. Chakeres and E. B. Royer,** "*The Utility of Hello Message for Determining Link Connectivity*", Proceedings of 5th International Conference on Wireless Personal Multimedia Communications (WPMC) Vol. 2 , PP. 504-508, Hawaii, 2002.

[4] **M. D. Naim Hider, M. D. Haque and M. D. Shohidul,** "*An Extensive Comparison among DSDV, DSR and AODV Protocols in MANET*", International Journal of Computer Application, Vol. 15, No.2, PP. 123-130, February 2011.

[5] **A. Iwata, C. Chiang, G. Pei, M. Gerla, and T. Chen,** "*Routing Strategies for Ad-hoc Wireless Networks*", IEEE Conference on Selected Areas in Communications, Vol. 17, No. 8, PP. 1369-1379, Japan, August 1999.

[6] **Noor Mohammad Suryati, Usop Azizol Abdullah, Ahamed Faisal Amri Abidin,** "*Performance Evaluation of AODV, DSDV and DSR Routing Protocols in Grid Enviornment*", International Journal of Computer Science and Network Security, Vol. 9, No. 7, PP. 45-53, July 2009.

[7] **P. Johnson, T. Larson, N. Headman, B. Mielczarek and M. Degmark,** "*Scenario Based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks*", Mobicom'99, PP. 195-206, 1999.

[8] **H. Zou, Q. Wei,** "*Efficiency Evaluation and Comparison of Routing Protocols in MANETs*", In Proceedings of ISISE-2008 Vol. 2, PP. 201-206, Japan, 2008.

[9] **G. S. Mamatha and Dr. S. C. Sharma,** "*Analyzing the MANET Variations, Challenges, Capacity and Protocols Issues*", International Journal of Computer Science & Engineering Survey (IJCSES), Vol.1, No.1, PP. 10-16, August 2010.

[10] **C. Mbarushimana, A. Shahrabi,** "*Comparative Study of Reactive and*

Proactive Routing Protocols Performance in Mobile Ad-hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), IEEE Computer Society, PP. 57-588, March 2007.

[11] **Haidar Safa, Hassan Artail and Diana Tabet**, "*A cluster-based trust-aware routing protocol for Mobile Ad-hoc Networks*" , Springer Wireless Network (2010), 16:969–984, DOI 10.1007/s11276-009-0182-1.

[12] **Fenye Bao, Ing-Ray Chen and Moonjeong Chang,** "*Hierarchical Trust Management for Wireless Sensor Networks and Its Application to Trust-Based Routing*", SAC'11, March 21-25, 2011, TaiChung, Taiwan., ACM 1978-1-4503-0113-8/11/03

[13] **Azzedine Boukerche, Yonglin Ren, and Richard Werner,** "*An Adaptive Computational Trust Model for Mobile Ad-hoc Networks*", IWCMC'09, June 21–24, 2009, Leipzig, Germany, ACM 978-1-60558-569-7/09/06.

[14] **Wenjia Li, Anupam Joshi and Tim Finin,**" *Automated Trust Management for Mobile Ad-hoc Networks Using Support Vector Machine*", IEEE 978-0-7695-4436-6/11, MURI FA9550-08-1-0265 2011DOI 10.1109/MDM.2011.21.

[15] **Christos Papageorgiou, Tasos Dagiuklas and Stavros Kotsopoulos,** "*Dynamic trust establishment in emergency ad hoc networks*", IWCMC '09, June 21-24, 2009, Leipzig, Germany. ACM 978-1-60558-569-7/09/06.

[16] **Pushpita Chatterjee,** "*Trust Based Clustering and Secure Routing Scheme for Mobile Ad-hoc Networks*", International Journal of Computer Network and Communication (IJCNC), Vol. 1, No. 2, July 2009.

[17] **A.Pravin Renold and R. Parthasarathy,** "*Source based Trusted AODV Routing Protocol for Mobile Ad-hoc Networks*", ICACCI'12, August 3-5, 2012, ACM 978-1-4503-1196-0/12/08.

[18] **S. Aruna and Dr. A. Subramani,** *Comparative Study of Weighted Clustering Algorithm for Mobile Ad-hoc Networks*, International Journal of Emerging Technology and Advance Engineering, ISSN 2250-2459, ISO 9001:2008, Certified Journal Vol. 4, Issue 5, May 2014.

[19] **Floriano De Rango and Salvatore Marano,** "*Trust-based SAODV Protocol with Intrusion Detection and Incentive Cooperation in MANET*", IWCMC'09, June 21–24, 2009, Leipzig, Germany.

[20] **V. Preetha and Dr. K. Chitra,** *Clustering and Cluster Head Selection Technique in Mobile Ad-hoc Networks*, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, ISSN (Print): 2320-9798, Vol. 2, Issue 7, July 2014.

[21] **N. Gupta, M. Shrivastava and A. Singh,** "*Cluster Based On-Demand Routing Protocol for Mobile Ad-hoc Network*", IJERT, Vol. 1, Issue No.3, 2012

[22] **Marc Bechlar and Hans-Joachim Hof and Denial Kraft and Frank Pahlke and I ars Wolf** "A Cluster Based Security Architecture for Ad-hoc Networks, in Proc of IEEE INFOCOM 2004.

[23] **Basant Kumar Verma and Dr. Binod Kumar,** "A Survey On Cluster Based Network For Ad-hoc Network", International Journal of Research in Computer Engineering and Electronics, ISSN 2319-376X, Vol. 3, Issue 5, PP. 1-5, Sep 2014.