RECENT TRENDS TOWARDS MULTIMEDIA BASED WIRELESS NETWORKING PROTOCOLS

Shivani
M.Tech Research Scholar, GIMET, Amritsar, India
(Sharmashivani1388@yahoo.com)

Er. Gagandeep Singh Saini
Assistant Prof., GIMET, Amritsar, India

Abstract

The fast development in network multimedia tools have let extra real-time digital companies such as for instance as an example video-conferencing, online games and distance knowledge to cultivate to be the standard internet tasks. These companies often necessitate the fundamental process to provide multicast facility. The multicast describes the distribution of from merely a unitary node to level of destinations. These real-time companies have a stringent necessity of QoS factors like bandwidth, delay, jitter etc. to make sure clear, regular, and fair sign to the receivers. This paper has presented recent protocols which are used in multimedia networks to provide better services. This paper ends up with the suitable future directions to extend this work.

Keywords:- QoS, Wireless network, AODV, Multicast.

1. INTRODUCTION

Wireless networks are becoming ever more popular and easy setting up. Although creating an instant network has become easier, doing it correctly remains as challenging. Wireless networks are now faster, have broader ranges, and are far more reliable than they used to be. they are also simple to hack, have problems with various from of interface, and can drop devices from the network if they're not setup properly. It's beneficial to have the help of an experienced network expert when implementing wireless network. If we've not network checked by a professional, it's very important to security and stability for network checked.

Wired networks will be the fastest and most reliable networks that may be implemented. They're not, however, easy to implement. Various wiring standards, the necessity for additional hardware, and complicated computer configurations require a specialist approach. Frequently enough homes and small offices are turning to wireless networks to supply blanket coverage with minimal costs and infrastructure, but wireless networks are frequently not properly secured, can lack speed, and can frequently fail from poor implementation or from interference. When we require the reliability, speed, and security of a wired network it's absolutely vital that consult a professional that could help plan and implement the network properly.
2. VARIOUS ROUTING PROTOCOLS
2.1 REACTIVE ROUTING PROTOCOLS
Reactive routing protocol is also known as on demand routing protocol and is based on Query-Reply topology [4]. In this protocol route is discovered whenever it is needed.

2.1.1 AODV
AODV (Adhoc On-demand Distance Vector) Protocol [8][4]: AODV protocol is proposed by C.E. Perkins and E.M. Royer and is combination of DSR and DSDV. It uses on demand mechanism of Route Discovery and Route Maintenance from DSR and hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. It is a beaconless protocol by which no HELLO messages are exchanged between nodes to notify them of these neighbors in the network. It uses destination sequence numbers to make certain loop freedom. The major vulnerabilities contained in AODV protocols are: Deceptive increase of sequence number and Deceptive decrease of hop count. AODV shares DSR’s on-demand characteristics in so it also discovers routes on an as needed basis with a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. That is in comparison to DSR, which could maintain multiple route cache entries for each destination. Without source routing, AODV depends on routing table entries to propagate an RREP back once again to the foundation and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to determine freshness of routing information and to prevent routing loops. All routing packets carry these sequence numbers. An essential feature of AODV could be the maintenance of timer-based states in each node, regarding using individual routing table entries. A routing table entry is expired if not used recently. Some predecessor nodes is maintained for each routing table entry, indicating the group of neighboring nodes which use that entry to route data packets. These nodes are notified with RERR packets when the next-hop link breaks. Each predecessor node, subsequently, forwards the RERR to its own group of predecessors, thus effectively erasing all routes utilizing the broken link. In contrast to DSR, RERR packets in AODV are designed to inform all sources using a link when a failure occurs. Route error propagation in AODV may be visualized conceptually as a tree whose root could be the node at the idea of failure and all sources utilizing the failed link because the leaves.

2.1.2 DSR
DSR (Dynamic Source Routing) [8] [4]: DSR protocol is proposed by D. B. Johnson, Maltz and Broch. DSR is based on source routing. In source routing, the sender of a bundle determines the complete sequence of nodes through that the packet must pass, the sender explicitly lists this route in the packet’s header, identifying each forwarding “hop” by the address of the following node to which to transmit the packet returning to the destination host. It's on the basis of the link state algorithm. Two basic parts of DSR protocol are: route discovery and route maintenance.

The important thing distinguishing feature of DSR is the utilization of source routing. That's, the sender knows the complete hop-by-hop path to the destination. These routes are stored in a route cache. The data packets carry the foundation route in the packet header. Whenever a node in the ad hoc network attempts to send a data packet to a destination which is why it doesn't already know the route, it runs on the route discovery process to dynamically determine this kind of route. Route discovery works by
flood the network with route request (RREQ) packets. Each node receiving an RREQ rebroadcasts it, unless it is the destination or it features a path to the destination in its route cache. This kind of node replies to the RREQ with a route reply (RREP) packet that's routed back once again to the initial source. RREQ and RREP packets will also be source routed. The RREQ accumulates the road traversed throughout the network. The RREP routes itself back once again to the foundation by traversing this path backward. The route carried back by the RREP packet is cached at the foundation for future use.

If any link on a source route is broken, the foundation node is notified using a route error (RERR) packet. The foundation removes any route applying this link from its cache. A brand new route discovery process must certainly be initiated by the foundation if this route remains needed. DSR makes very aggressive utilization of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any forwarding node caches the foundation route in a bundle it forwards for possible future use.

2.1.3 TORA
TORA (Temporary Ordered Routing Algorithm) [4]: TORA is manufactured by Park and Corson. It uses directed acyclic graphs (DAG) to define the routes either as upstream or downstream. This graph enables TORA to offer better route for networks with large population of nodes. When a link fails TORA has the capacity to patch itself around the purpose of failure but all the protocols have to re-initiate a route discovery. It involves four major functions: creating, maintaining, erasing and optimizing routes. TORA is just a distributed routing protocol predicated on a “link reversal” algorithm. It is designed to discover routes on demand, provide multiple routes to a destination, establish routes quickly, and minimize communication overhead by localizing algorithmic reaction to topological changes when possible. Route optimality (shortest-path routing) is considered of secondary importance, and longer routes tend to be used to steer clear of the overhead of discovering newer routes.

Those things taken by TORA could be described when it comes to water flowing downhill towards a destination node through a network of tubes that models the routing state of the actual network. The tubes represent links between nodes in the network, the junctions of tubes represent the nodes, and the water in the tubes represents the packets flowing towards the destination. Each node includes a height regarding the destination that is computed by the routing protocol. If a tube between nodes A and B becomes blocked in a way that water can't flow through it, the height of A is defined to a height greater than that of any one of its remaining neighbors, in a way that water will now flow back out of A (and towards the other nodes that were routing packets to the destination via A). When a node discovers a approach to a destination is no further valid, it adjusts its height such that it is just a local maximum regarding its neighbors and transmits an UPDATE packet. If the node has no neighbors of finite height regarding this destination, then your node instead attempts to find out a fresh route as described above. When a node detects a network partition, it generates a CLEAR packet that resets routing state and removes invalid routes from the network.

2.1.4 LAR
LAR (Location Aided Routing) [4]: LAR is proposed by Ko and Vaidya. The goal of LAR is to reduce the routing overhead by the use of location information. Position information is employed by LAR for restricting the flooding to a particular area. LAR designates two geographical regions for selective forwarding of control packets, namely, Expected Zone and Request Zone. The request zone is fixed from the source, and nodes that are not in the request zone do not forward a Route Request with their neighbors. The Expected Zone could be the region in that the destination node is likely to be present.

2.1.5 CBRP
CBRP (Cluster Based Routing Protocol) [4]: In CBRP, nodes are grouped into clusters. Each cluster has a bunch head that coordinated data transmission within the cluster and to other clusters. Only cluster heads exchange routing information as a result control overhead is far significantly less than flooding methods. The protocol suffers from temporary routing loops because nodes carry inconsistent topology information because of long propagation delays.

2.1.6 DYMO
DYMO (Dynamic MANET On-demand) [4]: DYMO routing protocol is successor of AODV protocol and shares lots of the benefits of AODV. Both basic operations of DYMO are route discovery and route maintenance. During route discovery, the originating node sends a Route Request (RREQ) through the entire network to find the target node. When the target node receives the RREQ, it
responds with a Route Reply (RREP) unicast toward the originating node. When the originating node receives the RREP, routes are established involving the originating node and the prospective node in both directions. DYMO uses sequence number to ensure loop freedom. It generally does not explicitly store the network topology; instead, nodes compute a unicast towards the desired destination only once needed.

2.2 PROACTIVE ROUTING PROTOCOL
Proactive routing protocol is also referred to as table driven protocol [8]. These protocols always maintain up-to-date information of the routes from each node to every other node in the network by exchanging topological information of the network nodes. Each node maintains a number of tables to store up to date routing information. Periodic route updates are exchanged to be able to synchronize the tables [4].

2.2.1 DSDV
DSDV (Destination Sequenced Distance Vector) [4]: DSDV is proposed by Perkins and Bhagwat. It is founded on distributed Bellman Ford Algorithm with improvements of freedom from routing loops. In this, each device maintains a routing table containing entries for all your devices in the network. In order to keep the routing table completely updated at all the time each device periodically broadcasts routing message to its neighbor devices. When a neighbor device receives the broadcasted routing message and knows the current link cost to the unit, it compares this value with the corresponding value stored in its routing table. If changes were found, it updates the worth and re-computes the length of the route which includes this link in the routing table.

The Destination-Sequenced Distance-Vector (DSDV) Routing Algorithm is based on the concept of the classical Bellman-Ford Routing Algorithm with certain improvements. Every mobile station maintains a routing table that lists all available destinations, the number of hops to attain the destination and the sequence number assigned by the destination node. The sequence number can be used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A place also transmits its routing table if a significant change has occurred in its table from the final update sent. So, the update is both time-driven and event-driven.

The routing table updates can be sent in two ways: - a "full dump" or an incremental update. A full dump sends the entire routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that's a full change since the final update and it must easily fit in a packet. When there is space in the incremental update packet then those entries may be included whose sequence number has changed. Once the network is relatively stable, incremental updates are sent in order to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps could be more frequent.

2.2.2 OLSR
OLSR (Optimized Link State Routing) [8] [4]: OLSR is proposed by Clausen and Jacquet. In this, MPR (Multipoint Relay nodes) are selected based on the greedy algorithm. MPR are accustomed to send control messages in the network to lessen overhead. The origin node select nodes as MPR which have reached one hop far from it and are able to cover the complete network. The source node communicates using its two-hop neighbors through these MPR. Nodes which are selected as MPR forward control messages in the network and the nodes that are not MPR but are one-hop neighbors just process the messages with forwarding them. It uses pure link state routing protocol. Optimizations are done in two ways: by reducing the size of control packets and by reducing the number of links useful for forwarding link state packets. OLSR is founded on three mechanisms: neighbor sensing, efficient flooding and computation of a maximum route using shortest path algorithm.

2.2.3 WRP
WRP (Wireless Routing Protocol) [8] [4]: WRP is proposed by Murthy and Garcia- Luna-Aceves. It is similar to DSDV protocol. The main goal is to steadfastly keep up routing information among all nodes in the network regarding the shortest distance to every destination. Each node in the network maintains four routing tables namely Distance table (DT), Routing table (RT), Link-cost table (LCT), Message retransmission list (MRL) table.

2.2.4 RIP
RIP (Routing Information Protocol) [1]: Routing Information Protocol (RIP) is an Interior Gateway Protocol used to switch routing information inside a domain or
autonomous system. RIP permits routers to switch information about destinations for the objective of computing routes through the entire network. Destinations may be individual hosts, networks, or special destinations used to convey a default route. RIP is based on the Bellman-Ford or the distance-vector algorithm and makes routing decisions based on the hop count between a modem and a destination.

2.2.5 STAR
STAR [4]: STAR is founded on link state algorithm. Each router maintains a source tree, which is really a set of links containing the most well-liked paths to destinations. Least overhead routing approach (LORA) can be used to lessen routing overhead and optimum routing approach can be used to obtain shortest way to the destination. Nearby source trees exchange information to steadfastly keep up up-to-date tables using link state update messages.

2.3 HYBRID ROUTING PROTOCOL
Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. So a Hybrid protocol is presented to overcome the shortcomings of both proactive and reactive routing protocols. Hybrid routing protocol is mixture of both proactive and reactive routing protocol. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. Hybrid protocol is suitable for large networks where many nodes are present [8].

2.3.1 ZRP
ZRP (Zone Routing Protocol) [4][8]: ZRP is proposed by Haas and Pearlman. In this network is divided into set of zones. The zone of a node is defined as the collection of nodes whose minimum distance from the node is not greater compared to the radius of the node. The minimum distance is defined with regards to amount of hops from that node. The routing within the zone i.e. intra-zone is done by utilizing proactive approach and routing beyond your zone i.e. inter-zone is done using reactive approach. For intra-zone routing a node got to know about its neighbors. The neighbors of nodes are defined as the nodes which are one hop away from particular node. The neighbor discovery is done by neighbor discovery protocol (NDP) so as to proactively monitor the network for intra-zone routing. The central 0-node selects its zone by considering set of nodes whose distance from the central node is not greater compared to the radius of the zone. These set of nodes are known as peripheral nodes. The intra-zone routing is done by intra-zone routing protocol (IARP). The inter-zone routing is done by inter-zone routing protocol (IERP). In the route discovery mechanism source nodes initiate the route discovery it first checks whether destination is within the zone or outside it, if it is within the zone then a route has already been obtained in the foundation node otherwise it send the query packet to its peripheral nodes, these nodes then verify if the destination is inside their zone or not. This way route discovery is been done.

2.3.2 ZHLS
ZHLS [4]: In ZHLS, network is divided into non-overlapping zones. Each node assigns an original ID and a zone ID. Two forms of link state updates used are node level LSP (Link State Packet) and zone level LSP. A node level LSP offers the node IDs of its neighbors in the exact same zone and the zone IDs of other zones. The same proactive and reactive approaches are useful for intra-zone and inter-zone routing. The origin node first checks its intra-zone routing table for the necessary destination. If the destination is based on its zone, the routing information has already been present.

2.4 ANT COLONY OPTIMIZATION
Ant colony optimization is a Metaheuristic technique of finding the suitable solution on the basis of the natural behavior of ants including their mechanism of cooperation and adaptation. In the beginning, the ants wander randomly. When an ant finds a source of food, it walks back once again to the colony leaving “markers” (pheromones) that report the road has food. When other ants run into the markers, they will likely follow the road with a certain probability. When they do, then they populate the road with their own markers while they bring the food back. As more ants find the road, it gets stronger until there are always a couple streams of ants visiting various food sources nearby the colony. The ACO algorithm is dependant on following three things.

i. Each path accompanied by the ant is associated to the candidate solution.

ii. The quantity of pheromone deposited is proportional to the grade of corresponding candidate solution of the mark problem.

iii. When you can find several path, the ant chose the road with an increase of pheromones deposited on it.
2.5 PARTICLE SWARM OPTIMIZATION

Particle swarm optimization is a computational method that optimizes a problem by iteratively trying to enhance a candidate solution with respect to confirmed way of measuring quality. PSO optimizes a problem by having a population of candidate solutions, here dubbed particles, and moving these particles round the search space in line with the simple mathematical formulae that specifies the particle’s position and velocity. Each particle’s movement is influenced by its local best known position but, can be guided toward the most effective known positions in the search-space, which are updated as better positions are found by other particles. That is expected to move the swarm toward the most effective solutions. A fundamental variant of the PSO algorithm works by having a population (called a swarm) of candidate solutions (called particles). These particles are moved around in the search-space according to a few simple formulae. The movements of the particles are guided by their own best known position in the search-space as well as the whole swarm’s best known position. When improved positions are increasingly being discovered these will likely then come to guide the movements of the swarm. The procedure is repeated and in so doing it is hoped, but not guaranteed, that a satisfactory solution will eventually be discovered.

3. LITERATURE SURVEY

S. Wong et al. [1] formulated a story graph optimization problem, called Minimal Gateway Assignment Problem, and proved so it was NP-hard. Nonetheless, they provided efficient algorithms to correct this dilemma with varying quantities of complexity and coordination. First, they provided a centralized polynomial-time algorithm that’s 2-approximable, and a distributed algorithm. Second, by simulation, they revealed that their centralized and distributed algorithms could perform near the optimal. They also reported an appealing result that cooperation has been the important thing factor to create optimal outcomes - an easy algorithm with tight cooperation among MANETs gave far better outcomes when compared to a smart algorithm with loose cooperation. I. K. Tabash et al. [2] proposed a fuzzy inference system on the basis of the factors of expected throughput and actual throughput to dynamically adjust the congestion window size that cause improvement in the performance of TCP in MANETs. This proposed scheme didn’t depend on any explicit feedback from the network, it required only the sender side modifications. The simulation study of the ad hoc network in this work was regarding equal sharing of network bandwidth among multiple TCP flows. Through extensive simulations, the authors had shown that how many concurrent flows significantly affects the TCP performance. The proposed scheme achieved the specified goals of improved performance compared to other TCP variants. Ahmed Nabet et. al. [3] have proposed an efficient secure routing protocol, ASRP, to guarantee the routing security in ad hoc networks. ASRP is used to supply powerful security extensions to reactive AODV protocol centered on modified secure remote password protocol and Diffie-Hellman (DH) algorithm. Radhika Saini et al. [4] have presented the malicious behavior of the node and security solution to protect such behavior. Security solutions include cryptography, protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP). P. Kuppusamy et al. [5] have showed the characteristics of ad hoc routing protocols TORA, AODV, and OLSR on the basis of the performance parameters like, end–to–end delay, packet delivery ratio, routing overload by increasing quantity of nodes in the network. The performance of all protocols was almost stable in sparse medium with low traffic. The effect is that performance of TORA is much better for dense networks. The AODV is much better for moderately dense networks whereas the OLSR performs well in sparse networks. The near future work suggested that your time and effort is likely to be made to enhance ad hoc network routing protocol by tackling core issues. Onkar V. Chandure et al. [6] have proposed a mechanism for the detection and prevention of grayhole attack in mobile ad hoc network using AODV protocol. Based on the proposed mechanism, each node in the network maintains DRI table containing entries for its neighboring nodes. Predicated on entries in DRI table, suspected node is checked using cooperative node and when level of suspicion concerning the suspected node increases, a Malicious Node Detection procedure is activated. Shobha Arya et al. [7] have proposed an algorithm for detecting malicious nodes in mobile ad hoc networks. The proposed algorithm uses encryption, acknowledgement and principle of flow conversion approach for security against four attacks namely packet eavesdropping, message tampering, black hole attack and gray hole attack. Arnab Banerjee et al. [8] have proposed a routing scheme named Administrator and Trust Based Secure Routing (ATSR) in MANETs. The proposed scheme provides secure routing by using parameter, trust, an integer value, that helps in the selection of administrator inside the network for routing. In addition it implements message confidentiality and integrity. Shujun Bi (2012) [9] have concluded that each
protocol has its characteristics and its obvious performance is many different in numerous network environments through simulator NS2 beneath the Ad Hoc network simulation and through examining the stability, throughput, equity and other performance indicators to contrast the advantages and disadvantages of AODV and TORA routing protocols. We cannot say which protocol is the finest in a complete way. Ad Hoc is the 4th generation mobile communication technology, the view of it is excellent, but there are still many problems to be solved, but it will play an even more and more important role in the future communication field. RAJESWARI.M et al (2012) [10] has presented a whole study on the performance of ad hoc network routing protocols with two Mac layer models. The routing protocols utilized in this study are AODV and ZRP which cover a great mixture of proactive and hybrid routing protocols. The performance is checked on jitter, throughput, end-to-end delay and total packets received measuring metrics by varying the number of nodes in the network using QualNet 5.0.2 network simulator. This demonstrates the performance of ZRP is average in the cases. AODV performs good, So it’s done that for AODV ad hoc routing protocol is better. Puneet Dadral et al. (2012) [11] evaluate the simulation of MANET reactive routing protocols which can be AODV and DSR and TORA. Comparative analysis has been carried out on the basis of the results obtained by simulations with OFDM and Extended Rate PHY physical characteristics in OPNET Modeler version 14.5. Metrics used are Throughput, End to End delay, Routing load and Media Access Delay. It is concluded that the worth of all metrics is higher for Extended Rate PHY than OFDM for all the routing protocols of MANET. N.M. Chacko et al. [12] outlined several routing algorithms in MANETs. Mobile AdHoc Networks (MANETs) features a wide selection of applications, which range from everyday cellular phone application to mission critical military applications. MANETs have proved their necessity and the easy creating networks. Thus MANETs are incredibly popular for scenarios which are sensitive and urgent like disaster relief, military applications, etc. As the application kind of MANETs increases, the attacks on MANETs also increase. A vast range of research has been conducted to help keep routing in MANETs robust and secure. One of the major research area is routing privacy. Many routing solutions were proposed to keep up privacy. Location aided routing has a book idea; in which routing was done based on location information, therefore node identity wasn’t revealed. M. Gharib et al. [13] proposed a brand new probabilistic key management algorithm for large-scale MANETs. To the best of the knowledge, this is the very first method which probabilistically used asymmetric cryptography to regulate the keys in MANETs. In this algorithm, they stored only some keys in each node as opposed to all. They analytically proved that the network will remain linked to a greater probability significantly more than 99.99%. Furthermore, they analytically calculated the typical path length in the network and showed that this parameter would not have an important increment employing their algorithm. All analytical effects were also validated by simulation to create them dependable. W. Liu et al. [14] proposed a generalized i.i.d. mobility model, by which each node moves once after every and everytime slots, and remained static between two moves. To investigate the TD trade-off beneath the g.i.i.d. model, they developed a book multi-relay multi-hop (MRMH) scheme that exploited the opportunities of multi-hop transmissions after the network has been static. Furthermore, enable the multi-hop transmissions, they constructed a brand new percolation highway system, that’s not been found in the TD trade-off analysis for MANETs. Utilizing the proposed MRMH scheme, they developed and proved constructive bounds for throughput and delay in MANETs with various scales of f. Their constructive bound was asymptotically optimal for f = 1. H. Dahshan et al. [15] proposed a trust based threshold cryptography revocation scheme for MANETs. Of their proposed scheme, the master private key was to split into n pieces relating with a random polynomial. Each node in the proposed scheme was configured with a before joining the network. Meanwhile, the master private key could be recovered by combining any threshold t pieces predicated on Lagrange interpolation. Consequently, the proposed scheme improved the safety levels in MANETs. The proposed hop-by-hop certificate revocation scheme was predicated on both threshold cryptography and transitive trust between mobile nodes. As a result of decentralized nature of the proposed scheme, it enabled several legitimate nodes to complete fast revocation of a nearby misbehaving node. The proposed scheme was highly robust in the mobility environment of MANETs. The benefits of the proposed scheme were justified through extensive simulations. S.Tan et al. [16] proposed a mechanism that provided Secure Route Discovery for the AODV protocol (SRD-AODV) in order to prevent black hole attacks. This mechanism required the inspiration node and the destination node to verify the sequence numbers in the Route Request (RREQ) and Route Reply (RREP).
messages, respectively, predicated on defined thresholds before establishing a reference to a destination node for sending the data. The simulation results utilising the Network Simulator 2 (NS2) demonstrated a noticeable difference in the ratio of packet delivery for three different environments employing their mechanism as set alongside the conventional AODV protocol. A black hole attack is one type of malicious attack that can be easily employed against data routing in MANETs. A black hole node replies to route requests rapidly with the shortest path and the maximum destination sequence number. The black hole node does not require an active route to a specified destination related to it and it drops the majority of the data packets so it receives. Reza Malekian et al. [17] have reviewed two routing protocols in mobile ad hoc networks i.e., AODV and OLSR and then compare them with regards to performance. This concludes that the OLSR enhances the end-to-end delay at the very least 22% when compared to AODV. Although, OLSR decreases overhead of network, it desires more resources such as for example bandwidth than AODV protocol because it must maintain the routing tables for several possible routes. Thriveni H.B et al. [18] have studied and analyzed the impact of variations in node velocity and node density combined with the selection of routing protocol, on network performance. We have selected Destination-Sequenced Distance Vector (DSDV) which really is a proactive routing protocol, and Dynamic Source Routing (DSR) which really is a reactive routing protocol, for the study. The network performance is measured with regards to Packet Delivery Ratio (PDR), End-to-End Delay and Throughput. The simulations are carried out in NS2.34. It may be observed from obtained results that DSR protocol outperforms DSDV protocol for chosen scenario specifications. D. Loganathan et al. [19] have reviewed the Multicast Parameters Based DSDV Routing protocol and scheduling algorithm for selecting the perfect path in the network nodes and along with various other QoS parameters requirement. This is observed that Multicost Parameters Based DSDV protocol outclasses is much better because it's high packet delivery ratio and less dropped packets when nodes have high mobility. K. Chen et al. [20] proposed a P2P content-based file sharing system, namely SPOON, for disconnected MANETs. The device used a pastime extraction algorithm to derive a node's interests from its files for content-based file searching. For efficient file searching, SPOON groups common-interest nodes that frequently meet with one another as communities. It took benefit of node mobility by designating stable nodes, which had the most frequent connection with community members, as community coordinators for intra community searching, and highly mobile nodes that visit other communities frequently as community ambassadors for intercommunity searching. An interest-oriented file searching scheme has been proposed for high file searching efficiency. Additional strategies for file pre-fetching, querying-completion, and loop-prevention, and node churn consideration were discussed to simply help expand increase the file searching efficiency. They first tested their system on the GENI Orbit test bed with a genuine trace and then conducted event-driven check out two real traces and NS2 simulation with simulated disconnected and connected MANET scenarios. The test results revealed that their system significantly lowered transmission cost and improved file searching success rate in comparison to current methods. S. Chadli et al. [21] made an intensive analysis of existing attacks. As a result of this they proposed a fresh system to classify attacks predicated on attributes that be seemingly the very best classification criteria to generate test-cases. They also applied the classification tree method (CTM) to choose test-cases to attack. Finally, they used the CTE (Classification Tree Editor) tool to generate and select test-cases. Due to the flexibility written by their dynamic infrastructure MANETs were vulnerable to types of security attacks. Furthermore, many conventional security solutions have now been developed. However, these proposals suffered from the difficulties of tests and evaluations. Among these solutions the intrusion detection systems (IDS). To enhance the caliber of protection of MANETs written by intrusion detection systems (IDS), they provided assessment of detection and test procedures far better.

5. CONCLUSION AND FUTURE SCOPE
From the survey, it has been concluded that the main element issue of QoS routing is to startup a multicast hierarchy which may meet specific QoS constraint. Nonetheless, the problem of making a multicast tree below numerous restrictions therefore can be obtained to be NP Complete. Thus, the issue is often resolved by heuristics or smart evolutionary optimization. Lately, some meta-heuristic methods like the ant colony algorithm, genetic algorithm and particle swarm optimization have now been applied by the analysts to eradicate the multi-constrained QoS routing problem. In near future we will enhance the multicasting further by using the clustering based techniques.
REFERENCES


