CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

Chapter 2 reviews the various studies carried out in the design of energy-efficient cluster-based routing schemes and secure routing schemes. The existing cluster-based schemes have been applied to offer efficient cluster formation for making energy efficiency. The review also focuses in detail on the security schemes for reducing malicious activities in a MANET to prolong the lifetime of the network.

2.2 MOBILE AD HOC NETWORK

Wireless networks and security might be considered an oxymoron. Indeed, it is hard to believe in security when it is so easy to access communication media such as wireless radio media. However, the research community in industry and academia has for many years extended wired security mechanisms or developed new security mechanisms and security protocols to sustain this marriage between wireless/mobile networks and security. Note that the mobile communication market is growing rapidly for different services and not only mobile phone services. This is why securing wireless and mobile communications is crucial for the continuation of the deployment of services over these networks. Wireless and mobile communication networks have had tremendous success in today’s communication market both in general or professional usage. In fact,
obtaining communication services anytime, anywhere and on the move has been an essential need expressed by connected people.

A MANET is an emerging type of wireless networking, in which mobile nodes associate on an extemporaneous or ad hoc basis. A MANET (Siva Ram & Manoj 2004) (Perkins 2001) is a self-organizing and self-configuring multi-hop wireless network, which comprises a set of mobile hosts that can move around freely and cooperate in relaying packets on behalf of one another. MANETs are self-forming and self-healing, enabling peer-level communications between mobile nodes without reliance on centralized resources or fixed infrastructure. These attributes enable MANET to deliver significant benefits in virtually any scenario that includes a cadre of highly mobile users or platforms, a strong need to share IP-based information, and an environment in which fixed network infrastructure is impractical, impaired, or impossible. In a MANET, multi-hop transmission (Xing & Wang 2011) facilitates forwarding packets from one node to the other nodes that may not be within the direct wireless transmission range of each other. Mobile nodes transmit the data on to the network. This transmission and receiving of data utilizes most of the energy of the network. So for better operation and increase the lifetime of the network, energy consumption must be the major factor of concern.

2.2.1 Routing Protocols in MANET

Ad hoc wireless networks perform the difficult task of multi-hop communication in an environment without a dedicated infrastructure, with mobile nodes and changing network topology. Different deployments exhibit various constraints, such as energy limitations, opportunities, such as the knowledge of the physical location of the nodes in certain scenarios, and requirements, such as real-time or multi-cast communication. One of the major technological challenges of such networks is that they require new
types of routing protocols. As opposed to the wired infrastructure, there are no dedicated router nodes: the task of routing needs to be performed by the user nodes, which can be mobile, unreliable and have limited energy and other resources. This section reviews the collection of technologies which have been proposed for routing in ad hoc networks (Azzedine et al 2011). The categories of ad hoc routing protocols is shown in Figure 2.1.

![Figure 2.1 Categories of ad hoc routing protocols](image)

2.2.1.1 Source-initiated routing protocols

Johnson et al (2001) proposed a most widely known routing algorithm, called Dynamic Source Routing (DSR) which is an ‘on-demand’ algorithm and it has route discovery and route maintenance phases. Route discovery contains both route request and route reply messages. In the route discovery phase, when a node wishes to send a message, it first broadcasts a route request packet to its neighbors. Every node within a broadcast range adds their node id to the route request packet and rebroadcasts. Eventually, one of the broadcast messages will reach either the destination or a node which has a recent route to the destination. Since each node maintains a route cache, it first checks its cache for a route that matches the requested
destination. Maintaining a route cache in every node reduces the overhead generated by a route discovery phase. If a route is found in the route cache, the node will return a route reply message to the source node rather than forwarding the route request message further.

The first packet that reaches the destination node will have a complete route. DSR assumes that the path obtained is the shortest since it takes into consideration the first packet to arrive at the destination node. Route reply packet is sent to the source which contains the complete route from the source to the destination. Thus, the source node knows its route to the destination node and can initiate the routing of the data packets. The source caches this route in its route cache. In the route maintenance phase, route error and acknowledgements packets are used. DSR ensures the validity of the existing routes based on the acknowledgements received from the neighboring nodes that data packets have been transmitted to the next hop. Acknowledgement packets also include passive acknowledgements as the node overhears the next hop neighbor is forwarding the packet along the route to the destination. A route error packet is generated when a node encounters a transmission problem which means that a node has failed to receive an acknowledgement. This route error packet is sent to the source in order to initiate a new route discovery phase. Upon receiving the route error message, nodes remove from their route caches the route entry using the broken link.

Ad hoc on-demand distance vector (AODV) (Perkins & Royer 1999) aims to reduce the number of broadcast messages forwarded throughout the network by discovering routes on-demand instead of keeping complete up-to-date route information. A source node seeking to send a data packet to a destination node checks its route table to see if it has a valid route to the destination node. If a route exists, it simply forwards the packets to the next hop along the way to the destination. On the other hand, if there is no route in
the table, the source node begins a route discovery process. It broadcasts a route request (RREQ) packet to its immediate neighbors and those nodes broadcast further to their neighbors until the request either reaches an intermediate node with a route to the destination or the destination node itself. The route request packet contains the IP address of the source node, current sequence number, the IP address of the destination node and the last known sequence number. An intermediate node can reply to the route request packet only if it has a destination sequence number that is greater than or equal to the number contained in the route request packet header. When the intermediate nodes forward route request packets to their neighbors, they record in their route tables the address of the neighbor from which the first copy of the packet has arrived.

This recorded information is later used to construct the reverse path for the route reply (RREP) packet. If the same RREQ packets arrive later on, they are discarded. When the RREP packet arrives from the destination or the intermediate node, the nodes forward it along the established reverse path and store the forward route entry in their route table by the use of symmetric links. Route maintenance is required if either the destination or the intermediate node moves away and it is performed by sending a link failure notification message to each of its upstream neighbors to ensure the deletion of that particular part of the route. Once the message reaches to source node, it then re-initiates the route discovery process.

Park & Corson (2001) proposed a Temporally Ordered Routing Algorithm (TORA). It is an adaptive and scalable routing algorithm based on the concept of link reversal. It finds multiple routes from a source to a destination in a highly dynamic mobile networking environment. In TORA control messages are localized to a small set of nodes nearby the topological change. Nodes maintain routing information about their immediate one-hop
neighbors. The three basic functions of the protocol are route creation, route maintenance, and route erasure.

Toh (1997) proposed an Associativity-based routing (AR) algorithm which considers route stability as the most important factor in selecting a route. Routes are discovered by broadcasting a broadcast query request packet. Using these packets, the destination becomes aware of all possible routes between itself and the source. The AR algorithm maintains a ‘degree of associativity’ by using a mechanism called associativity ticks. Each node maintains a tick value for each neighbor, which is increased by one every time a periodic link layer HELLO message is received from the neighbor. Once the tick value reaches a specified threshold value, it means that the route is stable. If the neighbor goes out of the range, then the tick value is reset to zero. Hence a tick level above the threshold value is an indicator of a rather stable association between these two nodes. Once a destination has received the broadcast query packets, it has to decide which path to select by checking the tick-associativity of the nodes. The route with the highest degree of associativity is selected since it is considered the most stable of the available routes.

Dube et al (1997) proposed a Signal stability-based adaptive routing (SSBR) protocol in which the main routing criteria are the signal and location stability. As in other on-demand routing protocols, the route request is broadcast throughout the network, the destination replies with the route reply message and then the sender sends data through the selected route. Additionally, the signal strength (link quality) between neighboring nodes plays a major role in the route selection process in this protocol.

Goff et al (2003) presented a preemptive routing in ad hoc networks. In conventional protocols, a path is considered broken only after several retransmissions have timed out. The algorithm attempts to initiate the
discovery process of an alternate route just before the probable route failure. The algorithm generates a preemptive warning when the signal power of the packet received drops below a predefined preemptive threshold. The correct setting of the preemptive threshold is the main challenge of the algorithm. If the value is too high, unnecessary warnings may be generated which can lead to greater overhead, unnecessary route discoveries and switches to possibly lower quality paths. On the other hand, if the value is too low, the path breaks much earlier than the alternate route is selected. This leaves a short time period for building an alternate path. As temporary channel fading can often create a weak reception without leading to route failure, the algorithm uses successive “query” packets to decide whether the generated warnings are valid.

Rosati et al (2008) proposed a Distributed ant routing (DAR) algorithm based on ant behavior in colonies. Ant colony optimization algorithms have been widely used in MANETs and the authors aim to design an algorithm incorporating the salient features of many existing approaches. The main design goal of DAR is to minimize the computation complexity. Each node contains routing tables which are stochastic with the next hop being selected based on weighted probabilities. These probabilities are calculated based on pheromone trails left by ants. Forward ants are used to find new paths. If multiple paths are available at a node, the next hop could be selected either randomly or the most optimal one. DAR mostly uses hop-by-hop optimal forwarding with the forward ant routed at each node based on probabilities for the next hop. Data packets are forwarded deterministically by selecting the highest probability at every node on the path. Thus, a global route is created by using local hop-by-hop information.

Naserian & Tepe (2009) proposed a Forwarding Dilemma game (FDG) approach to forwarding flooding packets in MANET with AODV as
the underlying routing protocol. The game is played within the network only when a node receives a HELLO or any other flooding message since the nodes are the players. The game, called the forwarding dilemma game is composed of the number of players receiving the packet, the forwarding cost and the network gain factor and it offers primarily two strategies forwarding or dropping the packet. Using a mixed strategy Nash equilibrium, the probabilities of forwarding the flooding messages are calculated. The FDG is implemented in AODV with the existing HELLO messages used in neighbor discovery. Since the HELLO messages are forwarded only to the winners of the game, the number of nodes participating in the route discovery process is reduced. The structures of the RREQ and RREP packets of AODV have been modified for the calculation of the probability of packet forwarding.

Lai et al (2007) proposed an Adaptive backup routing (ABR) that used the concept of backup routes to AODV. It sets up a mesh and multipath routing using RREP messages and aims to reduce control overhead. The mesh structure is created by overhearing data packets transmitted from the nodes in the neighborhood. This helps in reducing control messages and also reacts faster to the topology changes. Whenever a link break is detected at a node, the node itself initiates a handshake procedure with its neighbors and repairs the broken route. Backup route request (BRRQ) and backup route reply (BRRP) messages are used in the route repair process. The authors also suggest combining AODV-ABR with local route repair once the route breaks by broadcasting a RREQ message from the node with the broken link.

### 2.2.1.2 Table-driven routing protocols

Table driven protocols always maintain up-to-date information of routes from each node to every other node in the network. Routing information is stored in the routing table of each node and route updates are propagated throughout the network to keep the routing information as recent
as possible. Different protocols keep track of different routing state information; however, all of them have the common goal of reducing route maintenance overhead as much as possible. These types of protocols are not suitable for highly dynamic networks due to the extra control overhead generated to keep the routing tables consistent and fresh for each node in the network.

Perkins & Bhagwat (2001) introduced a Destination-Sequenced Distance-Vector (DSDV). As many distance-vector routing protocols, it relies on the Bellman-Ford algorithm. Every mobile node maintains a routing table which contains the possible destinations in the network together with their distance in hop counts. Each entry also stores a sequence number which is assigned by the destination. Sequence numbers are used in the identification of stale entries and the avoidance of loops. In order to maintain routing table consistency, routing updates are periodically forwarded throughout the network. Two types of updates can be employed; full dump and incremental. A full dump sends the entire routing table to the neighbors and can require multiple network protocol data units.

Incremental updates are smaller and are used to transmit those entries from the routing table which have changed since the last full dump update. When a network is stable, incremental updates are forwarded and full dump are usually infrequent. On the other hand, full dumps will be more frequent in a fast moving network. In addition to the routing table information, each route update packet contains a distinct sequence number assigned by the transmitter. The route labeled with the most recent sequence number is used. The shortest route is chosen if any two routes have the same sequence number.

Clausen et al (2001) presented an Optimized link state routing (OLSR) algorithm which improves on the classical link state protocols
through several optimizations targeted towards wireless ad hoc networks. These optimizations are centered on specially selected nodes called multipoint relays (MPR). First, only MPR’s forward messages during the route information flooding process, substantially reducing the total number of messages forwarded. In addition, link state information is generated only by the MPRs, further reducing the amount of data which needs to be disseminated. Finally, the MPRs might choose to report only links between themselves and their MPR selectors. This last technique of partial link state information is a departure from the customary approach of link state protocols which relay on the dissemination of the full link state.

Chiang et al (1997) proposed a Cluster head gateway switch routing (CGSR) protocol which uses a distributed algorithm called the Least Cluster Change (LCC). By aggregating nodes into clusters controlled by the Cluster Heads (CHs), a framework is created for developing additional features for channel access, bandwidth allocation and routing. Nodes communicate with the CH which in turn communicates with other CHs within the network. The selection process of a CH is an important task since changing CHs frequently adversely affect the resource allocation algorithms. Thus, cluster stability is of primary importance in this scheme.

The LCC algorithm is considered stable since the CHs change only under two conditions: when two CHs come within the range of each other or when a node gets disconnected from any other cluster. CGSR is an effective way for channel allocation within different clusters by enhancing spatial reuse. Each cluster is defined with unique Code Division Multiple Access (CDMA) code and hence each cluster is required to utilize spatial reuse of codes. Within each cluster, Time Division Multiple Access (TDMA) is used with token passing. Gateway nodes are members of more than one cluster; therefore, they need to communicate using different CDMA codes based on
their respective CHs. The main factors affecting routing in these networks are token passing and code scheduling. A packet is routed through a collection of these CHs and gateways in this protocol.

Murthy & Garcia-Luna-Aceves (1996) proposed a Wireless routing protocol (WRP) which builds upon the distributed Bellman-Ford algorithm. The routing table contains an entry for each destination with the next hop and a cost metric. The route is chosen by selecting a neighbor node that would minimize the path cost. Link costs are also defined and maintained in a separate table and various techniques are available to determine these link costs. To maintain the routing tables, frequent routing update packets must be forwarded to all the neighbors of a node and contain all the routes in which the node is aware of. Since these are just update messages, only the recent path changes are included instead of the whole routing table. To keep the links updated, empty HELLO packets are forwarded at periodic intervals only if no other updates messages need forwarding.

Chen & Gerla (1998) proposed a Global state routing (GSR) protocol, where the control packet size is adjusted to optimize the MAC throughput. Each node maintains the neighbor list and three routing tables containing the topology, the next hop, and the distance respectively. The neighbor list contains all neighbors of the current node. The topology table contains the link state information and a timestamp indicating the time in which the link state information is generated. The next hop table contains a list of next hop neighbors to forward the packets while the distance table maintains the shortest distance to and from the node to various destinations. A weight function computes the distance of a link which may be replaced by other QoS routing parameter. Initially each node in the network starts with an empty neighbor list and a topology table. It learns about its neighbors by the sender field of the incoming packets. By processing these packets to obtain
link state information, the best route to the destination is computed. After all the routing messages are processed, the routing table is created and shared with other nodes by broadcasting it to the next hop neighbors. This process is carried out periodically to maintain the most up-to-date information.

2.2.1.3 Hybrid routing protocols

The hybrid routing schemes combine elements of on-demand and table-driven routing protocols. The general idea is that area where the connections change relatively slowly are more amenable to table driven routing while areas with high mobility are more appropriate for source initiated approaches. By appropriately combining these two approaches the system can achieve a higher overall performance.

Samar et al (2004) designed a Zone routing protocol (ZRP) for large scale networks. The protocol uses a pro-active mechanism of node discovery within a node’s immediate neighborhood while inter-zone communication is carried out by using reactive approaches. Local neighborhoods, called zones, are defined for nodes. The size of a zone is based on q factor defined as the number of hops to the perimeter of the zone. There may be various overlapping zones which help in route optimization. Neighbor discovery is accomplished by either Intra-zone Routing Protocol or simple Hello packets. Intra-zone Routing Protocol is pro-active approach and always maintains up-to-date routing tables. Since the scope of Intra-zone Routing Protocol is restricted within a zone, it is also referred to as “limited scope pro-active routing protocol”. Route queries outside the zone are propagated by the route requests based on the perimeter of the zone, instead of flooding the network. The Inter-zone Routing Protocol uses a reactive approach for communicating with nodes in different zones. Route queries are forwarded to peripheral nodes using the border cast resolution protocol.
Pei et al (2000) proposed a Fisheye State Routing (FSR) protocol which takes inspiration from the ‘fisheye’ technique of graphic information compression. When adapted to a routing table, this technique means that a node maintains accuracy distance and path quality information about its immediate vicinity, but the amount of detail retained decreases with the distance from the node. Each node considers a number of surrounding fisheye scopes, areas which can be reached with 1, 2 . . . hops. A higher frequency of update packets are generated for nodes within smaller scope while the updates are fewer in general for farther away nodes. Each node maintains a local topology map of the shortest paths which is exchanged periodically between the nodes. With an increase in size of the network, a ‘graded’ frequency update plan can be adopted across scopes to minimize the overall overhead. This approach makes FSR an implicit hierarchical protocol. Its main advantage is the significant reduction of the control overhead.

Pei et al (2000) proposed a Landmark ad hoc routing (LANMAR) which builds subnets of groups of nodes which are likely to move together. A landmark node is elected in each subnet, similar to FSR. The LANMAR routing table consists of only the nodes within the scope and landmark nodes. During the packet forwarding process, the destination is checked if it is within the forwarding node’s neighbor scope. If so, the packet is directly forwarded to the address in the routing table. If a packet on the other hand is destined to a farther node, it is first routed to its nearest landmark node. As the packet gets closer to its destination, it acquires more accurate routing information, thus in some cases it may bypass the landmark node and routed directly to its destination. During the link state update process, the nodes exchange topology updates with their one-hop neighbors. A distance vector, which is calculated based on the number of landmarks, is added to each update packet. As a result of this process the routing tables’ entries with smaller sequence numbers are replaced with larger ones.
Wang et al (2009) introduced a Hybrid ant colony optimization (HOPNET) algorithm which is based on Ant Colony Optimization (ACO) and zone routing. It considers the scenario of ants hopping from one zone to the next with local proactive route discovery within a zone and reactive communication between zones. The algorithm borrows features from ZRP and DSR protocols and combines it with ACO based schemes. The forward ants are sent only to border nodes. These forward ants are then directed towards the destination node by using the nodes’ local routing table. The ants move from one zone to another via border nodes and by using available local routing information. The zone approach achieves the scalability. Link failures are handled within a zone without flooding the network. Inter and intra zone routing tables are always maintained which can efficiently rediscover a new route in case of a link failure.

2.2.1.4 Power-aware routing protocols

Power-aware routing makes the routing decisions dependent on considerations of the available energy of the nodes. These considerations can be significantly more complicated than simply finding the route with the lowest energy consumption. The protocols from this class take into consideration both the heterogeneity of the energy resources of the nodes, as well as the uneven energy consumption due to the topology of the network and the nature of the data flows. For many of these protocols, the ultimate objective is to maximize the lifetime of a network with nodes with limited and fixed energy resources.

Avudainayagam et al (2003) proposed a Device and energy-aware routing (DEAR) for a heterogeneous network where some nodes are on battery power while other nodes are connected to a continuous supply of power. The goal of the protocol is to rely on the latter type of nodes for most of the routing functionality, thus extending the lifetime of the battery powered
nodes. The DEAR protocol calls a node device-aware if it can distinguish between whether it is battery powered or externally powered and the cost of using a device of the latter type is zero. The routing table of device-aware nodes has an additional field called Device Type which indicates whether the destination node is on battery power or is externally powered. An additional redirect table contains pairs of destination addresses and redirect addresses. After every routing table update, the node calculates the least cost to any externally powered device from its routing table and updates the redirect table accordingly as well. During routing, the node compares the cost of reaching the destination versus the cost of reaching a powered node, and if the latter is cheaper, it will redirect the packet to a powered node. The DEAR protocol assumes that any powered node can boost its transmission power such that it is at a one-hop distance to any destination, thus the transmission from the powered node is considered to be of zero cost from an energy consumption point of view.

Scott & Bombos (1996) proposed a routing and channel assignment for low power transmission in PCS which uses a technique for minimizing the transmission power in Personal Communications Service networks by the simultaneous choice of the route and channel assignment. The aim is to increase the lifetimes of the individual nodes, and hence the network lifetime. The approach chosen is similar to the frequency reuse factor in Advanced Mobile Phone System cellular service. Due to the inherent complexity and the overhead involved with the continuous optimization of the entire network, the authors use an approach which is triggered only when new calls are made. In this least disturbance approach, new calls are placed such that the total power required to sustain the new call is minimal. This will minimize the new call’s interference with the rest of the network.
Chang & Tassiulas (2000) presented an Energy conserving routing in wireless ad hoc networks. The authors start with the observation that in general, the routes with the lowest energy cost are the routes with the least hops. It would appear that calculating the shortest path would also minimize the energy use. However, this technique leads to high energy consumption of the nodes which are along the shortest paths, while the battery power of the other nodes in the network remains largely unutilized. The authors introduce a routing strategy to maximize the network lifetime based on sets of source-destination pairs and the traffic generation rates on these flows. A class of flow augmentation and flow redirection algorithms are proposed which balance energy consumption rates in relation to the energy resources of the nodes.

Mohanoor et al (2009) proposed a Online energy aware routing which uses the polynomial time combinatorial techniques to compute energy efficient routes in MANET. The aim is to select a route which strikes a balance between the residual energy, the minimum energy level of any node in the path and the energy consumed along a path. The network is considered as a graph with the edge weights being the energy required to transmit. The sum of all weights along a path corresponds to the total energy consumed along the path. The authors consider several algorithms, united by their reliance on a two phase computation. The first technique, called the shortest widest path works as follows. First, variant of Dijkstra’s algorithm is applied to the graph constructed as above, which searches for paths with the minimum residual energy. There can be several paths which satisfy this condition. In the second phase, the algorithm chooses from these paths the one which has the lowest energy consumption.
2.2.1.5 Hierarchical routing protocols

Traditional internet routing is natively hierarchical. The first approximation ad hoc networks route over a flat collection of nodes. As the networks grow in size, these approaches lead to increased routing table sizes and control packet overhead. Hierarchical ad hoc routing protocols build a hierarchy of nodes, typically through clustering techniques. Nodes at the higher levels of the hierarchy provide special services, improving the scalability and the efficiency of routing.

Iwata et al (1999) presented a Hierarchical state routing (HSR) which is based on multilevel clustering. The goal is to replace the flooding of the control information with a local collection of this information in the CH, followed by the propagation of this information to the other CHs. First, nodes form level 0 clusters based on physical proximity and elect a CH. CHs connect to each other using virtual links. Multiple CHs can assemble themselves into higher level clusters. When a node changes its position, link state information is exchanged between CHs using the virtual links. The CH collects link state information about the nodes in its cluster and propagates it to other CHs through gateway nodes.

Routing in HSR happens using a hierarchical addressing scheme, with the CH acting as routers. When a node wants to send a packet, it sends it first to the local CH. The CH looks up the destination and sends the packet to its nearest gateway node. The gateway node then propagates the packet to the nearest gateway node at the next level of the hierarchy. The process continues until the packet reaches the gateway node of the destination cluster. The final gateway node routes the packet to the CH of the destination cluster which then forwards the packet to the destination node.
Sivakumar et al (1999) proposed a Core-extraction distributed ad hoc routing (CEDAR) which allows the consideration of QoS requirements in an ad hoc setting. The protocol selects a subset of nodes called the core of the network. Control messages will only be broadcasted among the nodes of the core, which can use any existing ad hoc routing mechanism for communication. The core is positioned as a ‘self-organizing routing infrastructure’ which performs route availability computations through waves of messages with dynamically limited propagation speed. The availability of increased bandwidth is transmitted by slow propagating increase waves, while information about decreased bandwidth is transmitted by fast propagating decrease waves. Routing in the CEDAR architecture happens as follows.

The source node sends a route request packet containing the source, destination, and the requested bandwidth to its dominator, the local core node. The dominator then computes and establishes a QoS route if feasible. The dominator nodes in each cluster maintain local state information and communicate with each other using virtual links. Route computation is carried out only on the core path. CEDAR aims more at robustness than optimality in computing the routes. Each core node only knows about the neighboring core node and has no global knowledge about the core sub-graph. This simplifies the maintenance of the core network which can be necessary due to topology changes induced by the mobility or failure of nodes. Core paths are established on-demand for connection requests and route computation is carried out only when a specific request for a route is received.

Eriksson et al (2004) proposed a dynamic addressing approach to improve scalability in ad hoc networks. The approach is based on adding a location based dynamic address to the node, in addition to its permanent identifier. A distributed lookup table is used to map the permanent identifier to the dynamic address. The main challenge is the assignment and
maintenance of dynamic addresses, which is done through a hierarchical address tree. The approach had been shown to successfully scale to networks of several thousands of nodes.

2.2.1.6 Multicast routing protocols

Multicasting is the simultaneous transmission of data from one sender to multiple receivers. Several widely used applications require multicasting at least at the logical level. Examples include audio–video teleconferencing, real time video streaming and the maintenance of distributed databases. In many cases it is advantageous to implement multicasting at the level of the routing algorithm.

Das et al (2002) proposed a Dynamic core based multicast routing (DCMP) which has been designed from the ground up as a multicast protocol, without relying on existing unicast protocols. DCMP classifies the sources into active, core active, and passive. Active sources use the traditional technique of flooding the network with JoinReq control packets at regular intervals. Nodes which desire to join the multicast group as a destination, reply with a JoinReply packet along the reverse path to the source. Passive nodes do not participate in the creation of the multicast routes themselves. Instead, a subset of the active nodes, the core active nodes forms a shared mesh through which the passive sources transmit their data packets. A single core active source can support a maximum of Max-PassSize passive sources and the hop distance between these sources is limited by the MaxHop parameter.

Li et al (2007) proposed an Energy efficient multicast routing. By assigning the transmission power of each node as a weight, the network graph is transformed to a new graph with weights between edges. The minimum energy multicast problem is to find the multicast tree whose total energy cost
is minimized. The problem now reduces to the directed Steiner tree problem. This is a known NP-hard problem, and the authors show that it is unlikely that there is an approximation algorithm with a constant performance ratio to the number of nodes in the network. The authors show several heuristic approaches for the problem. In the node-join-tree algorithm a cover set containing all non-leaf nodes is built incrementally by selecting the shortest path from the source node to the nodes in the uncovered set. The heuristic grows the multicast tree by selecting the nodes with the highest energy efficiency. The authors describe a distributed implementation of the algorithm where nodes have information only about their neighbours.

Randaccio & Atzori (2007) proposed a Genetic algorithms for group to the problem of finding multicast trees which optimize bandwidth and delay parameters. The algorithm is initialized by building a population of multicast trees in isolation by combining unicast paths between the source and destination pairs. The unicast paths follow the shortest path in terms of hops, calculated using Dijkstra’s algorithm. From this initial population, the GA algorithm generates various combinations and selects them for fitness. The fitness function used by the GA is based on the weighted average of transmission delay and network resource utilization.

Pompili & Vittucci (2006) presented a Probabilistic predictive multicast algorithm (PPMA). It improves the robustness and reliability of multicast trees in the event of link and/or node failures. The algorithm defines a new way to quantify the suitability of a link, the probabilistic link cost which is comprised of three terms: energy, distance and lifetime. Using this new metric, the multicast trees can be computed in the centralized or distributed manner. In the centralized approach, the algorithm simply substitutes the new metric for the other metrics traditionally used in the centralized Bellman-Ford algorithm. In distributed PPMA, the multicast tree
is created based on a private and a public link costs. The private link cost is used by the nodes which are already added to the multicast tree, while the reminder of the nodes in the network, used the public link cost to aggregate paths and form multicast trees.

Gui & Mohapatra (2006) proposed a Hierarchical multicast techniques and scalability. It introduces a framework for hierarchical multicasting in MANET. The proposed approaches include a domain-based and an overlay-driven. In the domain-based scheme, a large multicast group of nodes is divided into sub-groups. Each sub-group is assigned as a sub-root, chosen based on topological optimality. The sub-root uses its own lower-level multicast protocol to create its tree and deliver packets to nodes within its sub-group. The source nodes of each group and sub-roots form a special sub-group for upper level multicast which is used by the source node to deliver packets to the sub-roots. In the overlay-driven multicast scheme, a hierarchical overlay multicast protocol is used to construct the virtual multicast tree. In this framework, the upper level multicast tree needs to be logically spanned over all the group members. Once the tree is constructed, each non-leaf node is responsible to forward packets to its children in the tree. This mechanism further improves the data delivery efficiency.

Sun & Li (2006) proposed a QoS aware multicast routing which describe a series of QoS. The approach uses the delay, bandwidth and packet-loss characteristics with no additional signaling. It also incorporates multicast routing capability with the existing unicast. A source node sends a QoS route request, RREQ, which is forwarded by intermediate nodes until it reaches the destination. The destination sends back the RREP packet with a delay time corresponding to a predefined node traversal time (NTT). Intermediate nodes add their own NTTs to the delay value and update their routing tables. Routes with the minimum delay are selected for data transmissions. A similar
technique is applied for the bandwidth requirement where source nodes indicate their bandwidth requirements and intermediate nodes compare their available bandwidth before forwarding the packet.

Ji & Corson (2001) proposed a Differential destination multicast (DDM). In the DDM algorithm, the source node of a multicast transmission encodes all the destination addresses within each data packet header in an in-band fashion. With this approach, no fixed multicast tree is created, the routing will be soft-state, similar to state routing algorithms such as DSR. This allows a lower control overhead, as there is no need for extra packets to maintain multicast forwarding state. Control overhead only occurs when there is actual data to send. Nodes along the paths also do not need to maintain alternate backup routes. Once a node receives a data packet, it checks the DDM header to determine which node to forward the packet. This information will be remembered to help in the forwarding of future packets in the same direction. If a destination node changes, the upstream node informs all its immediate neighbours about the difference in the forwarding node.

2.2.1.7 Geographical multicast protocols

Geographical multicast routing is a variant of multicast where the goal is to route the packets coming from a source to destinations located within a specific geographical region. Naturally, for geocast to work, the nodes need to rely on localization techniques.

Liao et al (2000) proposed a geocasting protocol for mobile ad hoc networks based on GRID (GeoGRID). GeoGRID uses location information to define the forwarding zone. The geographic area of the network is divided into logical grids of size by d. In each grid area a gateway node is elected, whose responsibility is to forward the geocast packets. GeoGRID uses two geocast forwarding methods such as flooding based and ticket based. In
Flooding based GeoGRID, only gateway nodes within the forwarding zone are allowed to broadcast the geocast packets. In Ticket based GeoGRID, only selected gateways are allowed to forward the geocast packets. If the entire region is divided into an m by n region, a total of m + n tickets are first generated. The source then distributes these tickets evenly to neighboring gateway nodes in the forwarding zone which are closer to the geocast region than the source. The election of the gateway is an important issue in the GeoGRID protocol. The initial gateway of the grid is the node closest to the physical center of the grid. One way in which the gateway of a grid might change is when the gateway node moves out of the grid. Alternatively, a gateway node can silently turn itself to a non-gateway node and relinquish control to the other more suitable node who is then elected as the gateway.

Ko & Vaidya (2000) proposed a Geocasting in mobile ad hoc networks (GeoTORA) which builds upon the unicast TORA routing protocol. TORA uses the distributed “link reversal” algorithm and provides multiple routes to the destination. It also uses the concept of “heights” to determine direction of the links. In GeoTORA, the source node anycasts the geocast messages to the geocast group by using TORA. Once any node in the geocast region receives the geocast packet, it floods the packet into the region. This helps in limiting flooding only within its own region.

2.2.1.8 Location-aware routing protocols

Location-aware routing schemes in mobile ad hoc networks assume that the individual nodes are aware of the locations of all the nodes within the network. The best and easiest technique is the use of the Global Positioning System (GPS) to determine exact coordinates of these nodes in any geographical location. This location information is then utilized by the routing protocol to determine the routes.
Ko & Vaidya (2000) proposed a Location-aided routing (LAR) which utilizes location information to minimize the search space for route discovery towards the destination node. LAR aims to reduce the routing overhead for the route discovery and it uses the GPS to obtain the location information of a node. The intuition behind using location information to route packets is very simple and effective. Once the source node knows the location of the destination node and also has some information of its mobility characteristics such as the direction and speed of movement of the destination node, the source sends route requests to nodes only in the ‘expected zone’ of the destination node.

Since these route requests are flooded throughout the nodes in the expected zone only, the control packet overhead is considerably reduced. If the source node has no information about the speed and the direction of the destination node, the entire network is considered as the expected zone. A source node before sending a packet determines the location of the destination node and defines its ‘request zone’, the zone in which it initiates flooding with the route request packets. In some cases, the nodes outside the request zone may also be included. If the source node is not inside the destination node’s expected zone, the request zone must be increased to accommodate the source node. Also, a situation may occur where all neighboring nodes of the destination node may be located outside the request zone. In this case, the request zone must be increased to include as many neighbouring nodes as possible.

Basagni et al (1998) proposed a Distance Routing Effect Algorithm for Mobility (DREAM) which uses the node location information from GPS systems for communication. DREAM is a part proactive and part reactive protocol where the source node sends the data packet “in the direction” of the destination node by selective flooding. Each node maintains table with the
location information of each node and the periodic location updates are distributed among the nodes to keep this information as up-to-date as possible. Collectively updating location table entries indicates the proactive nature of the protocol while the fact that all intermediate nodes in a route perform a lookup and forward the data packet in the general direction of the destination, reflects DREAM’s reactive properties.

Giruka & Singhal (2007) proposed a On-demand geographic path routing (OGPR) which does not depend on a location service to find the position of the destination. OGPR is stateless and uses greedy forwarding, reactive route discovery and source-based routing. It is a hybrid protocol incorporating the effective techniques of other well known routing protocols for MANET. OGPR constructs geographic paths to route packets between a source and a destination node. A geographic path is termed as a collection of geographic positions from source to destination which decouple node IDs from the path, meaning that explicit node IDs are not used to construct a path. The addressing scheme is implemented by using a grid-based position encoding strategy. The entire network area is divided into square grids with a unit square grid assigned as an order-1 grid. Four adjacent order-1 grids form an order-2 grid and so on. With the grid structure set up, a unique binary address is assigned to all order-1 grids. Such a technique helps decouple node IDs from the addressing scheme and enables any node along the geographic path to forward data packets.

2.2.2 Applications of MANET

Military Scenarios: MANET supports tactical network for military communications and automated battle fields.

Rescue Operations: It provides Disaster recovery, means replacement of fixed infrastructure network in case of environmental disaster.
**Data Networks:** MANET provides support to the network for the exchange of data between mobile devices.

**Device Networks:** Device Networks supports the wireless connections between various mobile devices so that they can communicate.

**Free Internet Connection Sharing:** It also allows us to share the internet with other mobile devices.

**Sensor Network:** It consists of devices that have capability of sensing, computation and wireless networking. Wireless sensor network combines the power of all three of them, like smoke detectors, electricity, gas and water meters.

**Urban sensing:** This application area exploits the sensing and computation capabilities of smart phones, together with the wide range of their deployment in urban areas. Urban sensing is characterized by distributed sensing or data collection, and, in many cases, by distributed data customers. Smart phones can use both infrastructure based access and as well as ad hoc connections. Ad hoc approaches have the advantage of lower energy consumption, lower overall bandwidth consumption and improved privacy – but they inevitably involve more complex interaction patterns.

**Personal area networks (PAN):** This application area refers to networking among the portable devices carried by a single user. As long as these devices move with the user, this system can be considered as a local area network with the individual components being in a fixed relative position. The most popular current PAN technology is based on the Bluetooth standards. Quite often, one or more of these devices has its own internet connectivity through long range communication. Very similarly with the vehicular networks, aspects of ad hoc networking come into play when the personal networks of
different users will need to interact, or when devices of one users’ PAN needs to establish a short range communication with infrastructure elements such as when performing payment processing through near-field communication.

**Vehicular networking:** This area covers applications where one of the communication partners is a vehicle. This definition covers a very wide range of technologies. One type of vehicular networking involves the short range communication between the vehicle and personal devices carried by the passengers. The most widely deployed systems rely on Bluetooth, but other technologies, such as wireless fidelity (Wi-Fi) have also been suggested and implemented. Note that many devices, while connected to the local network of the vehicle, can also maintain long range wireless connections, for instance through 3G cellular telephony, and, increasingly, Worldwide Interoperability for Microwave Access (WiMAX) and Long-Term Evolution (LTE).

### 2.3 CLUSTERING IN MOBILE AD HOC NETWORK

Clustering (Dang & Wu 2010) is an effective topology control approach in MANET which can increase network scalability and lifetime. Node clustering is a very important optimization problem. In order to maintain a certain degree of service quality and a reasonable system lifetime, energy needs to be optimized at every stage of the system operation. A clustering scheme can effectively prolong the lifetime of MANET by using the limited energy resources efficiently.

In the MANET, mobile nodes can be grouped into small partitions which are called clusters. In each cluster, there is CH, also sometimes called as the leader, which coordinates data collection from the member nodes and transmission of the collected data to the other CH. CH selection can be done
in a centralized or distributed manner. In order to perform the MANET applications successfully, it is necessary to make energy efficiency in operation of MANET. Designing energy efficient cluster based routing for MANET is a great challenge. One way for preserving the energy during communication is by grouping the mobile nodes.

A MANET can also be divided into a hierarchical architecture by organizing nodes into clusters. Within each cluster, the information regarding the nodes and links is aggregated. Each cluster can thus be seen as a logical node at the cluster level. (Jane et al 2005) present various clustering schemes for MANET in which mobile nodes are divided into different virtual groups, and they are allocated geographically adjacent into the same cluster according to some rules with different behaviors for nodes. A typical cluster structure is shown in Figure 2.2.

It can be seen that the nodes are divided into a number of virtual groups based on certain rules. According to (Sakarindr & Ansari 2007), in a cluster structure, mobile nodes may be assigned a different status or function such as cluster head, cluster gateway, or cluster member. A cluster head normally serves as a local coordinator for its cluster, performing intra-cluster transmission arrangements, data forwarding and so on. A cluster gateway is a non-cluster head node with inter-cluster links, so it can access neighbouring clusters and forward information between clusters. A cluster member is usually called an ordinary node, which is a non-cluster head node without any inter-cluster links. The network layer only needs to maintain and manage the information of these logical nodes. The control overhead of the network is reduced with the aid of clustering.
2.3.1 Advantages of Clustering in MANET

Compared with routing in MANET, cluster based routing have a variety of advantages, such as more scalability, less load, less energy consumption and more robustness. In this section, the features (Parag Kumar 2013) as well as the objectives of MANET clustering is emphasized.

**Scalability:** In the clustering scheme, the mobile nodes are divided into a variety of clusters with different assignment levels. The CHs are responsible for data collection, information dissemination and network management. Clustering topology can localize the route set up within the cluster and thus reduce the size of the routing table stored at the individual nodes. Compared with a flat topology, this kind of network topology is easier to manage, and more scalable to respond to events in the environment.

**Less Load:** Many clustering routing schemes requires careful selection for clustering approach. For clustering topology, all cluster members only send data to CHs, and data aggregation is performed at the CHs, which help to dramatically reduce data transmission and save the energy. In addition, the
routes are set up within the clusters which thus reduce the size of the routing table stored at the individual nodes.

**Less Energy Consumption:** Clustering scheme helps to dramatically reduce the data transmission and save energy. Moreover, clustering with intra-cluster and inter-cluster communications can reduce the number of mobile nodes performing the task of long distance communications, thus allowing less energy consumption for the entire network. In addition, only CHs perform the task of data transmission in clustering routing scheme, which can save a great deal of energy consumption.

**More Robustness:** Clustering routing scheme makes it more convenient for the network topology control and it responds to the network changes. It comprises of node mobility and unpredicted failures. A clustering routing scheme only needs to cope up with these changes within the individual clusters, thus the entire network is more robust and more convenient for the management. In order to share the CH responsibility, CHs are generally rotated among all the nodes to avoid the single point of failure in clustering routing algorithms.

**Collision Avoidance:** In the multi hop flat model, the wireless medium is shared and managed by the individual nodes, thus this model can result in low efficiency in the resource usage. On the other hand, in the multi hop clustering model, a MANET is divided into clusters and the data communications between the mobile nodes comprise of two modes namely intra-cluster and inter-cluster respectively for data collection and for data transmission. Accordingly, the resources can be allocated orthogonally to each cluster to reduce the collision between the clusters and it can be reused cluster by cluster. As a result, the multi-hop clustering model is the appropriate model for large-scale MANET.
Latency Reduction: When a MANET is divided into clusters, only CHs perform the task of data transmissions out of the cluster. The mode of data transmissions only out of the cluster helps in avoiding collisions between the nodes. Accordingly, latency is also reduced. Furthermore, data transmission is performed hop by hop usually using the form of flooding in flat routing scheme, but only CHs perform the task of data transmission in clustering routing scheme, which can decrease hops from source to the destination, accordingly decreasing the latency.

Load Balancing: Load balancing is an essential consideration in the MANET. It aims at prolonging the network lifetime in MANET. Even distribution of the nodes among the clusters is usually considered for the cluster construction where CHs perform the task of data processing and intra-cluster management. In general, constructing equal-sized clusters is adopted for prolonging the network lifetime since it prevents the premature energy exhaustion of CHs. Besides, multipath routing is a method to achieve load balancing.

Fault-Tolerance: Due to the applicability of MANET in a many dynamic scenarios, the mobile nodes may suffer from the energy depletion, transmission errors, hardware malfunction and malicious attacks and so on. With applications such as surveillance and battle field envisioned to utilize a large number of mobile nodes, networks are prone to failure. The fault-tolerance is an important challenge. In order to avoid the loss of significant data from key nodes, the fault tolerance of CHs is usually required in these kinds of applications, thus effective fault-tolerant approaches must be designed in MANET. Re-clustering is the most intuitive method to recover from a cluster failure, though it usually disarranges the on-going operation. Assignment of CH backup is available scheme for recovery from a CH failure.
**Guarantee of connectivity:** A node in the MANET transmits the data to one or more destination through a single-hop or multi-hop routing, thus whether the data is successfully delivered or not to the destination is mainly determined by the connectivity of each node to its next hop node along the path. Furthermore, mobile nodes that cannot communicate with any other mobile node which will get isolated and their data can never be transmitted to the destination. Therefore, the guarantee of connectivity is an essential goal of clustering routing protocols in MANET.

**Energy-hole avoidance:** Generally, multi-hop routing is used to deliver the collected data to a destination. In those networks, the traffic transmitted by each node includes both self-generated and relayed traffic. Regardless of MAC protocols, the mobile nodes closer to the destination have to transmit more packets than those far away from the destination. As a result, the nodes closer to the destination tends to deplete their energy first, leaving a hole near the destination, partitioning the whole network, and preventing the outside nodes by sending the information to the destination, while many remaining nodes still have a plenty of energy. This phenomenon is called as energy hole.

**Maximizing the Network Lifetime:** Network lifetime is an inevitable consideration in MANET, because nodes are constrained in power supply, processing capability and transmission bandwidth. Usually, it is indispensable to minimize the energy consumption for intra-cluster communication by CHs which are richer in resources. Besides, mobile nodes that are close to most of the nodes in the clusters should be prone to be CHs. Additionally, the aim of energy-aware idea is to select those routes that are expected to prolong the network lifetime in inter-cluster communications, and the routes composed of nodes with higher energy resources should be preferred.

**Quality of Service:** The network applications and the functionalities of MANET prompt the requirement of quality of service (QoS). Usually,
effective sample, less delay and temporary precision are required. It is difficult for all the routing protocols to satisfy all the requirements of QoS, because some demands may breach one or more protocol principles. Existing clustering routing approaches in MANET mainly focuses on increasing the energy efficiency rather than the QoS support. QoS metrics must be taken into account in many real-time applications, such as battle-target tracking and emergent-event monitoring.

2.3.2 Clustering Attributes in MANET

Variability of Cluster Count: Based on the variability of the cluster count, clustering schemes can be classified into two types such as fixed and variable ones. In the former scheme, the set of cluster-head are predetermined and the number of clusters is fixed. However, the number of clusters is variable in the latter scheme, in which CHs are selected, randomly or based on some rules, from the deployed mobile nodes.

Uniformity of cluster sizes: In the light of uniformity of cluster sizes, clustering routing protocols in MANET can be classified into two classes like even and uneven ones respectively with the same size clusters and the different size clusters in the network. In general, clustering with different sizes clusters is used to achieve more uniform energy consumption and avoid energy hole.

Intra-cluster routing: According to the methods of intra cluster routing, clustering routing manners in MANET also include two classes namely single-hop intra-cluster routing methods and multiple-hop ones. For the manner of intra-cluster single-hop, all members in the cluster transmit the data to the corresponding CH directly. Instead, the data relaying is used when members communicate with the corresponding CH in the cluster.
**Inter-cluster routing:** Based on the manners of inter-cluster routing, clustering routing protocols in MANET include two classes such as single hop inter-cluster routing and multiple hop inter-cluster routing. For the manner of inter-cluster single-hop, all CHs communicate with the other CHs directly. In contrast to it, data relaying is used by CHs in the routing scheme of inter-cluster multiple-hop.

**Cluster head characteristics:** Based on the existence of cluster heads within a cluster, clustering schemes can be grouped into cluster head based and non-cluster-head based clustering. In the former schemes, there exist at least one CH within a cluster, but there is no CHs within a cluster in the latter schemes, such as some chain based clustering algorithms.

**Difference of capabilities:** Based on the uniformity of energy assignment for mobile nodes, the clustering schemes in MANET can be classified into homogeneous or heterogeneous ones. In homogeneous schemes, all the mobile nodes are assigned with equal energy, computation, and communication resources and CHs are designated according to a random way or other criteria. However, mobile nodes are assigned with unequal capabilities in heterogeneous environment, in which the roles of CHs are pre-assigned to nodes with more capabilities.

**Mobility:** According to the mobility attributes of CHs, the clustering approaches in MANET can also be grouped into mobile and stationary manners. In the former manners, CHs are mobile and membership dynamically change, thus a cluster would need to be continuously maintained. Contrary to it, CHs are stationary and can keep a stable cluster, which are easier to be managed. Sometimes, a CH can travel for limited distances to reposition itself for the better network performance.
Role: A CH can simply act as a relay for the traffic generated by the mobile nodes in its cluster or perform data collection in its cluster. Sometimes, a cluster head acts as a controller that takes actions based on the network conditions. It is worth mentioning, sometimes a CH acts in more than one role.

2.3.3 Clustering Process in MANET

Control manners: Based on control manners of clustering, clustering routing schemes (Lin & Gerla 1997, Zhengmin Kong et al 2010) in MANET can be grouped into centralized, distributed and hybrid ones. In centralized methods, a CH requires the global information of the network or the cluster to control the network or the cluster. In distributed approaches, a mobile node is able to become a CH or to join a formed cluster on its own initiative without global information of the network or the cluster. Hybrid schemes are composed of centralized and distributed approaches. In this environment, distributed approaches are used for the coordination between CHs, and centralized manners are performed for CHs to build individual cluster.

Convergence Time: Considering the convergence time, clustering schemes in MANET can be grouped into variable and constant convergence time ones. The convergence time depends on the number of nodes in the network in variable convergence algorithms, which accommodate well to small-scale networks. After a fixed number of iterations, constant convergence time algorithms certainly converge regardless of the scale of the networks.

Parameters for CH selection: Based on the parameters used for CH selection, the clustering approaches can be categorized as deterministic, adaptive, and random ones. In deterministic schemes, a special inherent attributes of the mobile nodes are considered, such as the identifier (ID), number of neighbors they have. In adaptive manners, CHs are elected from the deployed mobile nodes with higher weights, which includes such as
residual energy, communication cost, etc. In random modes, CHs are selected randomly without regard to any other metrics like residual energy, communication cost, etc. and it is mainly used in secure clustering algorithm.

**Proactivity:** According to the proactivity of clustering routing scheme, clustering routing schemes can be grouped into proactive, reactive, and hybrid ones. In proactive networks, all routes between source and the destination are computed and maintained before they are really needed regardless of the data traffic. Once a message arrives, it travels through a predetermined route to the destination. In contrast, no predetermined routes exist in reactive networks, in which the routing is chosen when a message needs to be delivered from source to the destination. Hybrid approaches use a combination of the above two ideas. For this kind of clustering routing, sometimes proactive clustering mode is adopted, but at other times reactive mode is used.

### 2.4 NEED FOR SECURE CLUSTER-BASED CLUSTERING SCHEMES IN MANET

MANET is a prevalent area of research which includes resource limitations, scalability, security and quality of service. Clustering algorithm (Dali Wei & Chan 2006) in a computer network is a division of the network into different virtual groups, based on rules in order to discriminate the nodes allocated to different sub-networks. The main goal is to achieve scalability in the presence of large networks and high mobility. Power failure of a mobile node not only affects the node itself but also its ability to forward packets on behalf of others and thus the overall network lifetime. A lot of work has been done to solve this energy awareness problem, the principal goal of which is the efficient use of energy by applying Dynamic Game Theory (Dayang Sun et al 2013)
In a MANET, power aware protocol (Shivashankar Varaprasad & Narayanagowda 2014) is an important issue to improve the communication energy efficiency at individual nodes. Energy consumption is a crucial design concern in MANET since nodes are powered by batteries with limited energy. Routing has become very important for exchanging information between people from / to anywhere at any time. Mobile nodes are battery-operated, and extending the battery lifetime has become an important aim. Most of the researchers have recently started to develop the power aware protocols (Shintre & Sondur 2014) for MANET. As each mobile node in a MANET performs the routing function for establishing communication among different mobile nodes, the ‘death’ of even a few of the nodes due to power exhaustion might cause a disconnect of services in the entire MANET. Thus, they suffer from limited energy level problems. Also, the nodes in the network are moving if a node moves out of the radio range of the other node, and the link between them is broken. Thus, in such an environment, there are two major reasons of a link breakage by node dying of energy exhaustion and node moving out of the radio range of its neighbouring node.

Energy efficient cluster-based approaches (Agarwal & Motwani 2009) are playing a crucial role in MANET. Cluster-based secure routing schemes (Yao & Lincong 2012) (Kadari et al. 2007) are providing a solution to address nodes’ heterogeneity, and to limit the amount of routing information that propagates inside the network. It increases the network lifetime, thus decreasing the amount of routing control overhead.

Clustering in MANET has many advantages compared to the traditional networks (Neha et al. 2012). It also helps to improve the network performance in terms of jitter, response time, throughput, delay and so on. The clustering mechanism provides an effective solution to enhance the network performance by using cluster-effective functions such as power
management, scheduling for channel access and coordination with the other clusters.

The characteristics of MANET such as open medium, dynamic topology, mobility and distribution of nodes make it more vulnerable to attackers that affect the functionality of the total network (Yu et al 2010). Providing security in MANET is an important aspect because of communications between mobile nodes are used in many critical applications. The great challenges of MANET are their vulnerabilities to various security attacks and inability to operate securely while preserving its resources. Ensuring secure communication (Lung-Chung Li & Ru-Sheng 2010) in MANET is extremely challenging because of the dynamic nature of the network and the lack of centralized management. For this reason, key management is particularly difficult to implement in such networks.

Hence, it is very much essential to develop effective intrusion-detection techniques to protect the nodes against attacks. So, an important issue to be focused when moving from a wired network to a wireless network is its energy efficiency and security issues. It is necessary to provide effective energy efficiency-based cluster and security schemes to enhance network management and routing.

2.5 CHALLENGES OF ENERGY-EFFICIENT CLUSTERING SCHEMES IN MANET

Cluster-based routing is proven as an effective concept to implement applications of a MANET. If the MANET under consideration is densely populated, then it is essential to organize the mobile nodes into clusters. This helps to achieve energy-efficient operations. Moreover, grouping nodes into clusters has been the most accepted approach to supporting scalability and energy-efficiency in the MANET. An energy-aware routing protocol
considers all nodes’ power during route establishment. Therefore, nodes that have higher power resources are given higher priority to participate in the routing process. Such a protocol should also ensure fair distribution of routing load among the nodes and wisely use all nodes' available power to prolong the network lifetime. Various mechanisms have been proposed to clustering for a MANET. This section reviews works regarding cluster-based routing schemes in the MANET.

Anupama & Bachala (2011) proposed schemes that focus on mobility-based cluster formation in MANET. These schemes are focused to form the clusters with stability. Jiang et al (1999) presented a Cluster-based Routing Protocol (CBRP) that used a min-ID algorithm to form stable clusters using local information. CBRP used two data structures for routing process that includes cluster adjacency table and the two-hop topology database that provide the features of route shortening and local repair. It performs well in a small network for making stable cluster.

Torkestani & Meybodi (2011) described weighted learning automata clustering algorithm for finding the node’s relative mobility with respect to all its neighbours. The highest expected weight is selected as cluster head. Bheemalingaiah & Naidu (2009) proposed an Energy Aware Cluster-based Multipath Routing (EACMR) that includes three phases such as cluster formation, cluster maintenance, and congestion control.

Gomathi & Rajendran (2012) proposed a cluster-based routing algorithm based on fuzzy logic that selects the appropriate path on a cluster-based multipath routing at fuzzy cost. Valentini et al (2013) surveyed on energy-efficient cluster-based power management technologies including static power management systems which utilized low power components and dynamic power management systems for optimizing energy consumption in the networks.
Sudipta et al (2012) presented a Weight-based Hierarchical Clustering Algorithm (WBHCA) for MANET that leads to a cluster formation and its stability by using combined weight metrics like highest heuristic degree, largest transmission range and low mobility factor. Saha & Chaki (2011) proposed a Cluster-Based Mobility Routing Protocol (CBMRP) for MANET that uses two metrics such as the node’s mobility and load-balance to select a cluster head.

Li & Wang (2010), presented a Cluster Cache Based K-hop Routing protocol, which used the cluster head cache to form clusters. (Majumder et al 2010) presented a Mobility-aware Clustering Scheme to form cluster. This scheme used priority-based algorithm to select a cluster head based on node degree, energy and mobility of nodes. This scheme does not perform well in a large network.

Chatterjee et al (2012) proposed a Secure Trusted Auction-oriented Clustering-based Routing Protocol that organized the network in 1-hop clusters. It used a secret voting scheme to elect trustworthy nodes as Cluster head. Tselikis & Mitropoulos (2012) proposed a Degree Based Clustering Algorithms for Mobile Ad Hoc Networks in which node degree, energy related fairness factor and security component and node’s Euclidean distance are taken into account to form clusters.

An energy-efficient variation of Optimized Link State Routing (OLSR) was proposed in Kunz (2008). This variation introduces two modifications to enhance the network lifetime such as the multi-point relays (MPR) selection criteria and the path selection algorithm. These modifications aim at avoiding the use of nodes with low residual energy level in the MPR set and to favor the selection of routes avoiding the use of exhausted nodes thus extending their existence in the network and the network life time. However, this approach did not provide a solution for the main drawback in


OLSR leading to a waste of nodes' energy because sending and receiving a large number of topology control messages were not eliminated. The routing concepts of OLSR were also used in Souto et al (2012) but with a new mechanism to calculate the routes and select the MPRs.

AlAamri et al (2010) proposed an On-demand Tree-based Routing Protocol (OTRP). This protocol combines the idea of hop-by-hop routing such as AODV with an efficient route discovery algorithm called the Tree-based Optimized Flooding (TOF) to improve the scalability of ad hoc networks when there is no previous knowledge about the destination. Route discovery overheads are minimized by selectively flooding the network through a limited set of nodes that are called branching-nodes because they form a tree-based structure to scan the network. Branching nodes, also called re-broadcasting nodes, are selected based on their locations that are obtained by using GPS. When a source node wants to communicate with a destination and no previous route exists, it divides its transmission area into four quadrants each of which has its own scanning process to re-broadcast Route Request (RREQ) packets.

The source node selects a branching node in each quadrant and appends to RREQ packet its own location and addresses of four branching-nodes that will re-broadcast the RREQ packet in the four quadrants. Upon receiving the RREQ packet, a node checks whether it is one of the branching-nodes indicated in the RREQ packet. If it is then it will process the packet and repeat the same procedure until reaching the destination, otherwise the packet is ignored. Processing the RREQ packet includes finding branching-nodes, updating the RREQ packet and then re-broadcasting it.

However, since each selected node does not broadcast RREQ packets back to the quadrant where the packet comes from, therefore it chooses only three branching-nodes to rebroadcast. Only the source node of
RREQ packet selects, at the beginning, four nodes for broadcasting the packet. If a node fails in selecting branching-nodes, then normal broadcasting will be carried. OTRP does not perform well in a heterogeneous environment as it selects re-broadcast nodes according to its location only. For example, if all branching-nodes are from the same type as the source node, then the destination that is from a different type cannot be reached unless all nodes are re-broadcasting. This means that OTRP will behave like AODV with higher overheads and delay where all nodes will re-broadcast to find a route.

2.6 SECURITY SCHEMES IN MANET

The characteristics of MANET pose great challenges with respect to security design because of their dynamic network topologies, lack of centralized control and self-organizing character. Collaboration between MANET nodes is the most problematic issue for forwarding packets between nodes. Each node can forward data packets to the other nodes. This makes it difficult to design secure routing. Secure routing plays a vital role in forwarding packets in critical applications. Node mobility creates more opportunities for various security attacks. Since the beginning of the mobile networking era, security has been part of the network architectures and protocol design even if it is considered to slow down the communication systems. Actually, network security is just a natural evolution of the security of stand-alone or distributed operating systems dealing with machine, network access control, authorization, confidentiality, etc. More precisely, it is about preserving the integrity, confidentiality and availability of resources and the network.

Security in a MANET is particularly difficult to achieve, notably because of the limited physical protection for each of the nodes, the sporadic nature of connectivity, the absence of a certification authority, and the lack of a centralized monitoring or management unit. Intrusion prevention is not
guaranteed to work all the time, and this clearly underscores the need for intrusion detection as a front-line security research area under the umbrella of MANET security.

Several security mechanisms have been developed such as authentication, encryption and access control others in order to offer secure communications over the network. According to the network environment, some security mechanisms are more mature than others due to the early stages of certain networking technologies such as wireless networks, ad hoc or sensor networks. However, even with maturity, and even if they are already widely implemented in marketed products, some security mechanisms still need some improvement. It is also important to consider the limited resources of mobile terminals and radio resources to adapt the wired network security mechanisms to a wireless context. These limited resources have a direct impact on security design for this type of networks.

In traditional wireless networks, mobile devices associate themselves with an access point which is in turn connected to other wired machines such as a gateway or a name server which handles network management functions. MANET, on the other hand, does not use such access points, and forms a completely distributed architecture. The absence of infrastructure and subsequently, the absence of authorization facilities, impede the usual practice of establishing a line of defense distinguishing nodes as trusted and non-trusted (Chatterjee 2009). There may be no ground for an a priori classification since all nodes are required to cooperate in supporting the network operation, while no prior security association can be assumed for all the network nodes. Freely roaming nodes form transient associations with their neighbours. They join and leave sub-domains independently with and without notice.
An additional problem related to compromised nodes is the potential Byzantine failures encountered within MANET routing protocols. In a Byzantine failure, a set of the nodes could be compromised in such a way that incorrect and malicious behavior cannot be directly noted at all. Malicious nodes can inflict a Byzantine failure on a system by creating new routing messages, advertising non-existent links and providing incorrect link state information. It can therefore be seen that intrusion prevention measures (Ming-Yang Su 2011) in MANET’s might prevent some attacks, but such measures are not enough. The Intrusion Detection System (IDS) (Azer et al 2008) is widely used in wired networks to protect networked systems once an intrusion is detected. However, techniques geared towards wired networks would not suffice for an ad hoc environment because of differences such as lack of fixed infrastructure, mobility, the vulnerability of wireless transmissions to eavesdropping and the lack of a clear separation between normal and abnormal behavior in a MANET. In addition, the MANET paradigm does not allow for the presence of traffic concentration points in the network, whereas most conventional IDS geared towards wired networks depend on such architecture.

Cooperation (Rashid et al 2008) between nodes is more challenging in MANET. Therefore, it is essential to develop an effective secure routing protocol to protect the nodes from anonymous behaviours. In general, malicious nodes do not want to forward a neighbour’s packets in networks that degrade the network performance. Existing schemes are not suitable for enhancing MANET security because of routing overhead and vulnerabilities. To minimize the activities of malicious nodes, they should be monitored continuously and not allowed to participate in routing. Security in MANET is a challenge for several applications. Game theory plays a significant role in providing security in MANET. (Roy et al 2010) surveyed the impact of the game theoretic approaches and their applications to network security. They
presented a taxonomy of game theoretic solutions to various security problems.

Game theory approach (Mohammad et al 2012) provides an effective solution to security problems in MANET; they prevent conflict in cooperation among the mobile nodes. They apply to a variety of disciplines including computer networks, economics, behavioural biology and political science as well. A Dynamic Bayesian Signalling Game allows a player with a number of possible actions to have a clear strategy for making an effective decision. In each message sent, the sender with a strategy must have a belief as to which node should receive it to ensure secure MANET routing. Various security mechanisms (Wu et al 2006) have been described for preventing nodes from attacks.

Ze Li & Haiying Shen (2012) used game theoretic approaches to analyse cooperation incentives for nodes provided by reputation systems and price-based systems. They addressed the issues of enforcing cooperation among selfish nodes and discriminating malicious nodes from regular nodes. This scheme does not sufficiently address security problems such as compromised cooperative nodes.

Mohammed et al (2011) proposed a protocol in which mechanism design theory is used to encourage nodes for participating honestly in the election process to balance the energy consumption. The incentives are based on the Vickrey, Clarke, and Groves techniques that ensure that truth-telling is the dominant strategy for any node in the clusters. It causes routing overhead as the cluster size increases. Haidar Safa et al (2010) presented a cluster-based trust aware routing protocol that used weighted degrees such as power consumption, neighbouring nodes, mobility and transmission power to form cluster head. It causes routing overhead due to the mobility of nodes.
Manshaei et al (2013) addressed the various research approaches in applying game theoretic methods to MANET network security. Several such approaches have been developed such as providing a certainty-oriented reputation system (Refaei et al 2010), reputation evaluation in hierarchical ad hoc networks (Yu et al 2010), preventing selfish and tariff free nodes (See Kee et al 2008) analysing the cooperation incentives for individual nodes (Liu et al 2005) detecting misbehaving nodes (Blanc et al 2005), analysing malicious behaviour (Theodorakopoulos & Baras 2007) investigating the interactions between nodes and providing incentives for good behaviour (Blanc et al 2005) and using a reputation system to enforce node cooperation (Michiardi & Molva 2002). According to (Buchegger & Boudec 2002) (Jochen & Boudec 2008), reputation systems reveal the truth about the other nodes based on reputation ratings and trust ratings.

Nabil & Hazem (2010) proposed a bidirectional authentication scheme in which authentication is considered to be a non-cooperative non-zero-sum bi-matrix game for Bluetooth devices. This mechanism alerts trusted Bluetooth devices of possible threats and malicious devices. This scheme is suitable only for short-range communication devices and is not scalable to long-range devices.

Nguyen et al (2014) proposed a secure many-to-many routing protocol for wireless sensor and actuator networks for providing both security and power efficiency. Security is achieved by using authenticated broadcast for task registration and secure multicast for data transmission. Power efficiency derives from the multicast nature of the communication. Lin et al (2014) proposed a Role-Based Privacy Aware Secure Routing Protocol to ensure privacy of information in Wireless Mesh Networks. It combines a dynamic reputation scheme with role-based multilevel security and a hierarchical key-management protocol to protect the nodes against internal
attacks. The dynamic reputation scheme cannot always encourage nodes to be cooperative.

Dingde Jian et al (2014) described a scheme for detecting traffic anomalies, including network faults, abuse and network attacks. They took network topology information into consideration and transformed domain analysis for finding abnormal components. Zhu et al (2012), described a collaborative Intrusion Detection System to analyse an incentive-based resource allocation problem. It needs enough credits to detect malicious nodes, otherwise it drops the packets.

Markus (2013) studied an infinitely repeated discounted game in which a player perfectly observes any other player’s action choice with a fixed and finite delay. This game has no pure strategy Nash equilibrium. Theodorakopoulos & Baras (2007) used a fictitious play game theory model to analyse malicious behaviour. They used the worst case equilibrium that gives the highest payoff for malicious users. Marcin (2012) introduced a procedural value for cooperative games to determine the sharing of marginal contributions to coalitions that are formed by players joining in random order. It allows false data injection into networks by compromised insiders eavesdropping data transmission.

Rafsanjani et al (2012) presented reputation schemes to perform the fast misbehaviour detection. This scheme does not perform well at finding a selfish node in high traffic. Kumar et al (2010) analysed the performance of the Ad hoc on-Demand Distance Vector (AODV) and CBRP. AODV discovers a route through network-wide broadcasting to provide reliable data transmission. The source host starts a route discovery by broadcasting a route request to its neighbours until it reaches the destination. On the route-request phase, there is a requested destination sequence number that is essential for the routing-loop problem. AODV causes high packet overhead to form a
routing path because of the larger flooding range, and it needs more time to recover false paths and to discover new paths. CBRP and AODV are not considered secure by preventing nodes from attacks.

Patcha & Park Daojing (2006) employed the signaling game to model the intrusion detection in the Ad Hoc networks where a host-based IDS is used, however, they did not thoroughly research into the game’s properties such as the equilibrium of the game.

2.7 SECURITY CHALLENGES IN MANET

Security challenges make it difficult to design secure routing in MANET. Yujun et al (2014) proposed a TOpology-Hiding multipath Protocol (TOHIP) that analyzed the threats of topology exposure. It provides the capability to find better routes. TOHIP has more routing overhead than secure routing protocol (SRP) when it is measured in bytes and it did not use any efficient security algorithm to prevent the attacks.

Ting et al (2014) applied the concept of dynamic secret to design an encryption scheme for smart grid wireless communication. It has good compatibility which could be integrated with many wireless techniques and applications. Since the length of retransmission sequences is used to generate the secret key, the attackers can hack that secret key very easily.

Shen & Zhao (2013) proposed an Anonymous Location-based and Efficient Routing protocol (ALERT) in order to provide high anonymity protection in a route with low cost. ALERT is not completely bulletproof to all attacks. The delay of ALERT increases slightly in the group movement model. ALERT’s random relay selection generates longer path length than the shortest path.
Ranjeet Kaur et al (2013) addressed the issues and challenges of the various multipath routing protocols in MANET. It ensures reliability, load balancing and Quality of Service (QoS). Multipath routing protocols have been proposed for MANET. They did not design a multipath routing protocol. They did not pay special attention to simultaneous use of paths, data forwarding mechanism considering the delay of the available paths, scalability and energy efficiency.

Ziming Zhao et al (2011) proposed a risk-aware response mechanism to systematically cope with routing attacks in MANET. A risk-aware response solution is used for mitigating MANET routing attacks. The experiment results clearly demonstrated the effectiveness and scalability of risk-aware approach. The mean latency of risk-aware response is higher than the other response mechanisms, when the number of nodes is minimized.

Defrawy & Tsudik (2014) addressed a number of issues arising in suspicious Location-based MANET (LAM) settings by designing and analyzing a privacy-preserving and secure link-state-based routing protocol. It is not suitable for large scale network to achieve scalability. Any node can lie about its location or generate multiple LAM as part of a Sybil attack.

Xin Ming et al (2011) proposed a novel route discovery mechanism based on the Estimated Distance to reduce the control overhead of Routing Protocols (EDRP) in MANET. The EDRP is used to reduce the routing control overhead by restricting the propagation range of RREQ packets. The packet delivery ratio and the average end-to-end delay give some negative effects when the node distribution is very sparse.

Djahel et al (2011) designed a cross layer scheme that ensures higher detection accuracy. They have designed a cross layer scheme that ensures higher detection accuracy. If no shared node is identified, then the
source node delays or abandons the transmission of the data packets, leading to a severe degradation of the network performance.

Mohamed Tekaya et al (2010) present a protocol named as QoS and Load Balancing-AOMDV, a solution to achieve better load balancing with respect to the end-to-end QoS requirement. If one RREP is received, therefore only one route layout from source to destination is used to send data packets. If many RREPs are received, the source chooses the best route based on the minimum hop count. They did not calculate any routing parameters like distance, energy and link quality to select the best path.

Yanbin Yang & Hongbin Chen (2009) proposed a protocol which introduces a stability factor which conserves and stabilizes energy among the nodes, and a delay reduction mechanism which reduces the average end-to-end delay of the network. The protocol does not perform packet delivery ratio while maintaining the other quality of service parameters. Energy consumption of network can be reduced by decrementing the transmission power of the nodes depending on the minimum distance required for communication and the energy level of nodes.

Chai Keong et al (2009), discussed the various load metrics and summarized the principles behind several existing Load-Balanced Ad hoc Routing protocols (LBAR). LBAR perform load balancing during route maintenance. But these protocols do not perform load-balancing during route discovery.

Prayag et al (2008) proposed a novel method of message security using trust-based multipath routing. They did not design a more efficient algorithm for selecting the routes from a set of routes. Strong encryption methodologies would be analyzed to provide a better security mechanism. They had compared with their results only those of dynamic source routing
protocol, but not with the other routing algorithms such as AODV and Temporally ordered routing algorithm.

Nait-Abdesselam et al (2008) devised an efficient method to detect and avoid wormhole attacks in the Optimized Link State Routing (OLSR) protocol. In OLSR, each node periodically sends routing control messages, which increases the load in dense networks. As these routing control messages are tunneled through the wormhole tunnel, the traffic increases dramatically, and congestion becomes inevitable through the path of that wormhole tunnel. This makes the legitimate nodes suspect and faultily identify some links as containing wormhole tunnels because of the increased delays.

Papadimitratos & Haas (2006) evaluated the Secure Message Transmission (SMT) protocol and the Secure Single Path protocol for malicious disruption of data transmissions. The security and fault-tolerance of the data communication are paramount in the inherently insecure and unreliable ad hoc networking environments. SMT with link state allows us to isolate the performance of SMT from the underlying routing protocol and to impose different limitations such as the number of available routes, delays, and overhead.

2.8 LOAD-BALANCING SCHEMES IN MANET

A MANET has important characteristics in terms of topology dynamics due to node movement. Load-balanced clustering schemes (Aoudjitat et al 2009) increase scalability and reduce the routing overhead in MANET. To achieve fairness and uniform energy consumption, an efficient clustering algorithm should produce load-balanced cluster head to adapt topology dynamics.
Hui Chenga et al (2013) formulated the dynamic load-balanced clustering problem into a dynamic optimization problem. They proposed to use a series of dynamic genetic algorithms to represent a feasible clustering structure in MANET. Its fitness is evaluated based on the load-balance metric. It is not focused on dynamic multi metric clustering problem.

Shengxiang Yang et al (2010) addressed the static shortest path problem using intelligent optimization techniques. They used GAs by immigrants and memory schemes to solve the dynamic shortest path routing problem in MANET. They designed a mechanism of the standard GA and integrated the several immigrants and memory schemes to enhance routing performance in a dynamic environment. These schemes are not applied to multicasting routing problem in dynamic network environments.

Bhaskar Nandi et al (2010) concentrated on the implementation of Weighted Clustering Algorithm with the help of Genetic Algorithm to improve the performance of the cluster head selection procedure. It used the combined weight metrics such as cluster head degree, battery power, node mobility and distance to search dominant set. This scheme selects the minimum number of cluster heads that covered all the nodes. GA does not provide an optimal solution when they decrease the transmission range because the number of cluster heads increased.

Bo Peng & Lei Li (2012) presented a new adaptive genetic simulated annealing algorithm for QoS multicast routing. The authors combine GA and SA by randomly altering symbols of the chromosome and then making successive random modifications. For a large scale network, it is time-consuming to obtain the optimal solution to the least cost QoS multicast routing problem.
Paul & Preetha (2013) described a novel method to cope with the dynamic nature of the MANET. The main idea is to cluster the networks by using avoidance strategy. It is neglecting the dynamicity of the sub networks during the leader election process. This enhanced the performance of leader election with respect to the network overhead. Topology tracing is done by flooding which consumes much of the network resources. They do not use the efficient scheme to trace the networks.

Ting Lu & Jie Zhu (2013) proposed an energy-efficient genetic algorithm to find the delay constrained multicast tree to reduce the power consumption. The proposed algorithm applied crossover and mutation operations on trees. The heuristic mutation technique can improve the total energy consumption of a multicast tree. This algorithm focuses only on source-based routing trees but not on shared multicasting trees.

Shea & Macker (2013) developed a new method for determining the number of clusters by using relative Eigen value quality. They designed a technique to minimize the multi way normalized cut, a metric that tries to simultaneously minimize the number of edges cut between clusters. This method is not suitable for updating the clustering in a distributed manner as the network evolves over time.

Syed Zohaib et al (2013) proposed the Optimizing Complex Cluster formation in MANET using SAT/ILP Techniques. The objective of this scheme was to avoid the broadcasting storm problem with the minimum number of transmissions. The objective of the ILP formulation was to find the minimum set of connected cluster heads. It takes more time to find optimal solution as the network gets bigger.

Peng Zhao et al (2013) developed a loose virtual-clustering-based (LVC) algorithm to construct a hierarchical network and to avoid packet
forwarding via high power nodes. It does not rely on geographic information or multi-radio multichannel. It is not focused on energy issues.

Gongqi Lin et al (2014) presented a new energy-aware Two Disjoint routing problem (EAR-2DP). The problem aims to reduce energy expenditure by maximally switching off unnecessary links during off-peak periods such that the remaining powered on links are sufficient to route traffic demands subject to two constraints such as link utilization and the minimum number of two disjoint paths used to route traffic demands. Extensive simulations on both real and synthetic network topologies and traffic demands have shown their benefits in reducing energy consumption while addressing critical network performances, such as link utilization, route reliability, and path length. It is not perform well in terms of route reliability.

Ibukunola et al (2013), described an energy function model based on Geographic Adaptive Fidelity for saving energy consumption in MANET. They used meta-heuristics mechanism for solving convoluted optimization problems by mimicking the biological evolution of a computing model. It minimizes the energy consumption by possible optimal solution. It does not perform well in large scale network structure.

### 2.9 MULTIPATH ROUTING IN MANET

Topological changes in MANET frequently render routing paths unusable. A suitable technique for addressing this problem is to enhance the diversity of paths between the source and destination. However, multipath routing is a challenging task. In particular, the correlation between the failures of the paths in a path set should be as small as possible. Shared nodes and links between the paths are usual failure points. Disjointed path sets require the multiple paths to be link-disjoint or node-disjoint. However, selecting an optimal path set is an NP-complete problem. Due to the dynamic nature of
network topologies and the resource constraints, routing in MANETs is a challenging task. Multipath routing can increase end-to-end throughput and provide load balancing in wired networks.

However, its advantage is not obvious in mobile ad hoc networks because the traffic flows along the multiple paths may interfere with each other. In addition, without accurate knowledge of topology, finding multiple node-disjoint paths is difficult. The multipath routing methods can reduce the frequency of route discoveries and balance network loads. The multipath routing technique has demonstrated its efficiency in improving MANET performance against the single path routing. In conventional networks like internet, the multipath mechanism has been utilized to offer load balancing and reliability of data delivery. In a MANET, multipath routing is developed according to primary motivations such as energy consumption, reliability and fault tolerance, load balancing, QoS improvement, and security.

Due to the resource limitations of MANET, intensive traffic loads in high-data rate applications are prone to congestion, which decreases the network performance. Hence, the multipath approach can benefit from the high density of MANETs to increase network throughput by employing more network resources. Furthermore, multipath routing can provide reasonable bandwidth requirements of different applications and reduce the probability of network congestion through splitting network traffic over multiple paths. Node-disjoint multiple paths are selected for data transmission to spread the load among different nodes that provide an effective load sharing mechanism among the multiple paths in MANET.

Multiple paths can be used as backup route or be employed simultaneously for parallel data transmission like round robin. The multiple paths obtained can be grouped into three categories such as disjoint, inter-twisted and hybrid paths.
1. **Disjoint:** This group can be classified into node-disjoint and link-disjoint. In the node-disjoint multipath type, there are no shared nodes between the calculated paths that links source and destination. The link-disjoint multipath type may share some nodes, but all the links are different.

2. **Inter-twisted:** The inter-twisted multipath type may share one or more route links.

3. **Hybrid paths:** The combination of previous two kinds. Of all the multipath types, the node-disjoint type is the most disjointed, as all the nodes / links of two routes are different in which the network resource is exclusive for the respective routes. Nevertheless, the pure disjoint approach is not always the optimal solution, especially for sparse networks and multi-criteria computing.

Most of the proposed multipath protocols (Tarique et al 2009) are based on the single-path version of an existing routing protocol such as AODV and AOMDV, DSR and SMR. Most of these protocols are based on a reactive routing protocol like AODV or DSR. In fact, reactive multipath routing protocols improve network performances such as load balancing, delay and energy efficiency, but they also have some disadvantages:

- **Route request storm:** Multipath reactive routing protocols can generate a large number of route request messages. When the intermediate nodes have to process duplicate request messages, redundant overhead packets can be introduced in the networks.

- **Inefficient route discovery:** To find node-disjoint or link disjoint paths, some multipath routing protocols prevent an intermediate node from sending a reply from its route cache. Thus, a source node has to wait until a
destination replies. Hence, the route discovery process of a multipath routing protocol takes longer compared to that of DSR or AODV protocols.

Compared to reactive routing, the proactive routing protocols need to send periodic control messages. Hence, several researchers consider proactive routing protocols as not suitable for ad hoc networks. For a network with low mobility and network load, the reactive routing protocols generate fewer control messages. However, given a network with high mobility and large traffic, the cost of route discovery and route maintenance will rise significantly. On the other hand, the proactive protocols try to keep a routing table for all possible destinations and therefore provide a transmission delay shorter than reactive routing protocols. Furthermore, because the proactive protocols try to maintain the information of the whole network by periodical control messages, they can discover multiple routes more efficiently without much extra cost.

Chen & Wu (2011) proposed an anonymous multipath routing protocol based on secret sharing. The protocol provides identity anonymity, location anonymity, data and traffic anonymity by employing cryptograph technology and secret sharing in MANET communication process. Meanwhile, a hash function is introduced to detect active attacks in the data transmission process. The protocol can effectively thwart various passive attacks and reduce the successful probability of active attacks. This scheme cannot thwart both the passive attacks and active attacks simultaneously.

Krishna et al (2012) proposed a quality of service enabled ant colony-based multipath routing (QAMR) algorithm based on the foraging behaviour of ant colony for selecting path and transmitting data. In this approach, the path is selected based on the stability of the nodes and the path preference probability. The authors have considered bandwidth, delay and
hop count as the QoS parameters along with the stability of node, number of hops and path preference probability factors.

Sheikhan & Hemmati (2011) proposed artificial neural networks as computational tools to solve constrained optimization problems. The use of Hopfield neural network as a path set selection algorithm is explored. Since this algorithm produces a set of backup paths with much higher reliability, it is beneficial for MANETs. The authors use link expiration time (LET) between two nodes to estimate link reliability. In this approach, node-disjoint and link-disjoint path sets can be found simultaneously with route discovery algorithm. So, if someone wants to find both node-disjoint and link-disjoint path sets, there is no need to submit extra control messages, as overhead, to the MANET. It can find path sets with higher reliability.

Cervera et al (2011) present a taxonomy of flooding disruption attacks that affect either the flooding of control traffic information or the selection of the MPRs in OLSR-based networks. All the multipath routing strategies based on the selection of MPRs as a flooding mechanism are susceptible to these attacks. The attacks have impact either in the topology discovery or route computation phases. Yi et al (2011) proposed a multipath extension to OLSR (MP-OLSR). MP-OLSR is a hybrid multipath routing protocol with multiple descriptions coding for data transfer. In MP-OLSR, the construction of multiple paths leverages on Dijkstra’s algorithm to find optimal routes in terms of hops.

The security attacks initiate serious routing malfunctions in the underlying network. Some attacks are less severe while some are more severe. For instance, selective forwarding attacks drop certain packets and forward the rest to the next hop, whereas sink-hole attacks drop all the packets without forwarding them, and thus create a Denial of Service circumstance that is difficult to confront. These network layer security attacks can be handled
through the development of appropriate secure routing protocols. The use of wireless communication makes the MANET more prone to security threats ranging from passive eavesdropping to active interference. Without proper security provisioning, nodes are easily captured, compromised, and altered by the malicious nodes. The design of an efficient routing protocol in MANETs has become a challenging problem. This kind of networks are more prone to both link and node failures due to restricted energy or mobility.

Additionally, when a node misbehaves during the execution of the routing protocol the connectivity of the network is compromised. Multipath routing has been proposed in MANETs to improve scalability, fault tolerance, security, load-balancing, energy-conservation and QoS. Unlike the single path strategy, in a multipath approach different paths are computed between a source and a destination to increase the routing resilience against failures. In multipath routing protocols there are three major challenges to be addressed: (a) discovery multiple routes (disjoint routes or routes with nodes or links in common), (b) path selection (multiple paths can be used as backups or simultaneously for parallel data transmission), and (c) load distribution (how data is transmitted through the multiple routes). So, it is essential to design the secure multipath routing schemes in MANET.