Arab American University – Jenin

Faculty of Graduate Studies

Connectivity and Reliability of Mobile Ad Hoc Networks

By

Salah Jabareen

Supervisor

Dr. Adwan Yasin

This thesis was submitted in partial fulfillment of the requirements for the master degree in Computer Science

November/ 2016

Connectivity and reliability of mobile ad-hoc networks

By

Salah Jabareen

This thesis was defended successfully on ………………………………… and approved by:

Committee Members	signature
1……………………………………	…………………………………….
2……………………………………	…………………………………….
3……………………………………	…………………………………….

اهـــداء

الى من مهدا لي طريق العلم بعد الله....

الى من ذللا لي الصعاب بدعواتهما الصالة....

الى من غرسا فيي حب العلم وكان لهما الفضل في بداية مشواري الذي اوصلني الى ما انا اليه....

الى والدي رحمهما الله وجعل بذور العلم التي زرعوها فيي في ميزان اعمالهم....

الى من صبر واحتمل معي ومنحني الفسحة والوقت... اخوتي الاعزاء...

الى اساتذتي الذين ما بخلوا علي بشئ من علمهم....

الى زملائي الذين كانوا بمقام الاخوة.....

اليهم جميعا اهدي هذا العلم المتواضع.....

الباحث

الشكر والتقدير

لا يسعني وانا اضع اللمسات الاخيرة لانهاء دراستي هذه الا ان اتقدم بالشكر والامتنان الى كل من قدم يد العون وكانت له مساهمة فيها, واخص بالشكر هنا استاذي د. عدوان ياسين المشرف على هذه الرسالة والذي كان له كل الفضل بعد الله عز وجل في انارة طريق البحث لي ومنذ بداية دراستي في برنامج الماجستير من خلال توجيهاته وارشاداته ومنحي شرف مشاركته في ابحاثه, جعلها الله في ميزان اعماله.

كما اتقدم بالشكر الى جميع المدرسين الذين درسوني خلال فترة دراستي خلال العامين الماضيين في برنامج ماجستير في علم الحاسوب في الجامعة العربية الامريكية في فلسطين ووضعوني على طريق العلم والبحث لتكون بداية لمستقبل ملئ بالبحث والانجاز والتميز كمان عودونا دائما.

والله ولي التوفيق

Abstract

Mobile ad-hoc networks is the base infrastructure for many useful applications. The protocols used in mobile ad-hoc networks are the base protocols for several applications like wireless sensor networks (WSN) which could be used in industry and monitoring purposes, VANET (vehicular ad hoc networks) which is a network of mobile vehicles. This type of networks has significant importance, and unique characteristic. MANET consists of mobile nodes that move in and out of the network in unorganized fashion, no central administration or infrastructure exists. As a result, the need to design a protocol that can provide the necessary reliability, connectivity, and security increases.

In this thesis we present current routing protocols under "FLAT class" category. Specially AODV, DSR, TORA, DSDV, OLSR and DYMO protocols. We experimentally evaluate 4 of these protocols and conclude comparison in performance and behavior under several scenarios like high mobility, high density, and also limited power nodes and others. We claim that current protocols are not enough to cube all the challenges and all conditions facing ad-hoc networking. And hence we add some contributions to enhance the reliability and connectivity of the current routing protocols.

In this thesis we proposed new routing algorithm that considers two of the major problems facing MANET networks, power and mobility. This algorithm is built based on the AODV routing protocol by modifying the optimal route selection scheme. The proposed algorithm considers the mobility and remaining energy instead of minimum number of hops. The simulations shows promising results as we will show next in chapter 6.

Table of Contents

Table of Figures

Table of tables

Chapter 1: Introduction

1.1 MANET:

The rapid increase in mobile devices development and technology advancements in wireless communications has made building applications an urgent need. More and more mobile devices like laptops, smartphones, robots, personal assistance devices and many more become popular and spread widely among people and connecting everywhere become a necessity. The need to stay connected all time despite the location and heterogeneity of infrastructures and devices quickly and in low cost and in different fields become an urgent requirement. MANET deals with this kind of needs.

Mobile ad hoc network (MANET) is a type of networks that uses wireless communications where no administration or central management and control unit exit like routers. In such cases where no administrator unit exits, nodes should act as routers capable to retransmit packets to their neighbor nodes within its transmission range. MANET does not depend on any pre-constructed infrastructure. Therefore, MANET can be deployed in locations where infrastructure does not exist like rescue operations, war fields, and isolated open areas.

MANET has certain characteristics; such as dynamic topology. The result of nodes mobility where nodes move in all directions and frequently change their locations causes the topology instability; this constraint represents a challenge for the routing protocol to be rapidly adaptive to topology change. MANET consists of mobile devices and are often limited in resources like processing, memory, storage, battery power and bandwidth. Because of such limitations, the routing protocol should minimize the traffic to the minimum.

Many routing protocols have been developed in mobile ad hoc networks, some protocols work in reactive manner where routing table is built upon request like AODV, DSR, and TORA. Some others use proactive manner where routing table is initially constructed and all nodes already knows the route for a specific destination, such protocols include OLSR, DSDV. Moreover, some protocols works on reactive and proactive way like DYMO.

The proactive protocols relay on periodic update and exchange of topology information. Nodes in MANET networks are capable to forward packets using up-to-date routing information. This periodic update and information exchange consumes the network and results in a remarkable network overhead when topology maintenance state depending on the protocol used and the degree of mobility. Reactive protocols prevent the periodic routing information exchange to save the network resources. Those protocols searches for paths and optimal routes upon request; that is, when any node needs to communicate and transmit data to any other destination node, the protocol initiates a route discovery message to look for available or optimal route then start sending data. Such protocols requires some time upon each request to build up the routing path which results in initial delay, the node have to wait some time until the route is found then start transmitting the data.

1.2 Problem statement:

Mobile ad hoc networks get more attention form research community because of its unique and challenging characteristics. Dynamic topology change, limited power resource, multi-hop, and mobility are complex features in MANET. Many protocols have been proposed to cube some or all of these features. The conventional routing protocols and mechanisms does not provide the appropriate way of discovering optimal routes or providing high quality and quantity of service in such high dynamic topologies as in MANET case. In this thesis, we will evaluate some of the conventional routing protocols that are developed for mobile ad hoc networks in terms of reliability and performance issues. Moreover, protocols may work fine and show good performance under optimal scenarios, in this thesis we will evaluate protocols under several extreme conditions and specific cases.

MANET protocols has several problems and still need enhancement, in this thesis, we will propose some enhancements and developments for the routing protocols so as to reach the desired performance for MANET. The suggested enhancement will be simulated and compared to traditional protocols.

1.3 Thesis Goals:

We aim after the end of this thesis to achieve the following goals:

1- Phase I: (data collection and analysis)
   a. Collecting information about MANET routing protocols and its implementations.
   b. Evaluating MANET routing protocols and concluding withdraws.
   c. Suggesting enhancements for MANET routing.

2- Phase II: (Simulating MANET protocols)
   a. Preparing the required simulation environment.
   b. Testing out MANET routing protocols performance under specific conditions and scenarios like (high density network, high degree of mobility, limited power etc.) using NS-2.35 simulator.
   c. Concluding the best protocol to deploy under specific conditions.

3- Phase III: (Routing Enhancement)
   a. Proposing new algorithm based on the results collected from simulating MANET routing protocols

b. Simulating the new algorithm and concluding results
c. Future work will be on security issues concerning MANET networks, suggesting new mechanisms to enhance security.

1.4 Thesis outline:

The rest of the thesis is organized as follows:

Chapter 2 Literature Review: this chapter provides a literature review of mobile ad-hoc networks definition, applications, some important concepts related to MANET, challenges in MANET networks, and finally MANET routing protocols classification.

Chapter 3 MANET routing protocols: 6 of the most common MANET routing protocols under "FLAT class" protocols which include: AODV, DSR, TORA, DSDV, OLSR and finally we introduce DYMO protocol are reviewed. We explain the routing algorithm and mechanism and the problems for each of these routing protocols.

Chapter 4 simulation setup: this chapter summarizes the simulation environment and the simulator specific characteristics and the parameters and metrics that will be used in testing and evaluating MANET routing protocols and the new proposed algorithm.

Chapter 5 Experimental Study: in this chapter we applied the simulation parameters and environment to the selected routing protocols, we selected AODV and DSR as reactive protocols, and DSDV and OLSR as proactive protocols. We also tested conditions like mobility, density of the network and power consumption. We then studied the results and concluded.

Chapter 6 Ways of enhancing Connectivity and reliability by considering mobility and power consumption: in this chapter we introduced a new algorithm that considers the nodes mobility and power consumption. The base idea for this algorithm is to calculate the link breakage time and selecting optimal route based on the estimated time for a link to be broken. Moreover the power level of intermediate nodes in the route also considered so as to guarantee fair load distribution among all nodes in the network. We tested this new approach and concluded the results.

1.5 Research methodology:

In this thesis we aim primarily to find out the problems concerning connectivity and reliability of MANET routing protocols, and we used two research methodologies to answer our questions about the performance of those protocols and what parameters could result in degradation in performance. We first used theoretical study and assumes several withdraws and next we tested out our assumptions using experimental tests using network simulator.

We gathered information about conditions that may influence performance of routing protocols by literature review most reliable approved routing protocols like (AODV, DSR, DSDV, TORA, OLSR, and DYMO). We focus our research to compare routing protocols in means of average throughput, average delay, packet delivery fraction, lifetime, and overhead, and experimenting different environment changes like network density, mobility, power consumption and density and how it affects the performance of routing protocols. The results are collected using NS-2.35 simulator which can support such protocols and gives the ability to create the required environment.

Chapter 2: Background and Literature Review

2.1 Mobile Ad Hoc Networking (MANET)

2.1.1 Definition

MANET [1], [2] networks is a very interesting topic in the research community. MANET is a type of wireless networks where devices in these networks has no central controlling unit like access points, MANET has dynamic topology, the nodes has no central infrastructure to operate their work. As a result, the nodes in MANET work as bridges capable to forward packets to their neighbors, and provides links to bypass messages to desired destinations. The MANET routing protocol needs to be efficiently implemented and handles routing tables in dynamic fashion to perfectly adapt to this dynamic topologies. Dynamic topological change in MANET requires rapid reconstruction of the routing tables because it is difficult to predict the changes in the topology; these changes occurs due to several originators, one is the limitations due to power sources of nodes, nodes movement, heterogeneity of nodes and unpredicted behavior [3].

MANET is different from the standard WLAN network is that there is no central administration and control unit (AP). Figure 2.1 represents an example of a standard wireless local area network and a typical mobile ad hoc network. The nodes in standard WLAN can communicate through the intermediate access point that has all required information for managing the nodes and facilitate the communication process, nodes in WLAN can’t communicate directly with each other and needs the assistant of the AP.

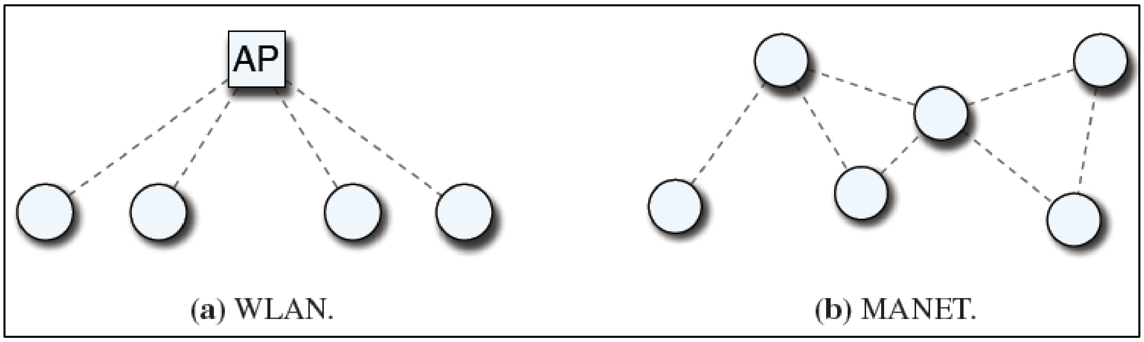


Figure 2. 1: MANET vs. WLAN Communication

On the other hand, the nodes in MANET needs the assistant of each other to communicate. The network needs to manage itself and be aware of the existence of each other. As a result of the distribution and movement of nodes, routing become a major issue in MANET. Moreover, as a result of mobility, the topology changes frequently and nodes keeps leaving and participating in the network. Also nodes population may vary from several nodes to hundreds. MANET used in several applications and the routing protocols needs to satisfy the required specifications for these applications. Several protocols were implemented to satisfy the unique characteristics of MANET.

2.1.2 MANET applications

Mobile ad hoc networks has significant important and could be applied in several applications: one is the Wireless Sensor Networks (WSN) which is a collection of autonomous sensors that cooperate together to perform specific tasks which is not possible in the traditional networks. Those sensors are placed in several environments and conditions to monitor some places and phenomena.

Another useful application of MANET is in the military applications like battle fields and critical situations where no central management unit exists or in regions where no communications like satellite or cell phones available. Another application is the rescue operations and disaster conditions and in scenarios where the communication infrastructure destroyed or unreachable.

A fourth area is the temporal connections that could be efficiently configured in special and temporal gatherings or groupings. For example a rapid network that provides internet connections in airports or in conferences or any group that wants to share resources temporarily. Establishing permanent network infrastructure in locations for temporal use is expensive and worthless, hence MANET solves this problem and provides the required service quickly and cost effectively.

Another application is the personal networks, each person could have several wirelessly enabled devices like mobile, laptop, watches and many others. MANET can provide a convenient medium to connect these devices.

MANET can be adaptively deployed in areas with no infrastructure, or inability to use any existing network, or even when we want to enlarge any existing network or when establishing new infrastructure is expensive and time consuming.

2.1.3 General concepts:

In MANET several concepts needs to be in mind as it has a specific unique specification when applied MANET:

- MANET routing

Routing in general refers to the process in which devices in a network can transfer data between each other. This process consists of two operations, (1) route discovery process and

(2) is the data transfer from source to destination throughout the network. The complex process in networking is to find the optimal route within a network, the cost effective route could be found using special algorithms that are appended in the routing protocols, the optimality of a route could be the usage of minimum hops to use to reach a desired destination. The information about the best paths to use produced by routing protocols algorithms are stored in routing tables which dynamically or statically contains all the reachable nodes stored as a list of IP addresses in the internetwork.

Routing in MANET has a unique characteristic compared to conventional wired networks. Mobile ad hoc networks are self-managed and multi-hop network, nodes are mobile and hence the topology frequently changes due to that mobility [4]. Devices in MANET acts as clients or routers that is capable of forwarding packets to other nodes [5]. No central management unit and hence there should be a reliable procedure as nodes may leave the network and new nodes may come into the network, this protocol must be able to find the optimal route appropriately.

- Protocol distribution

The protocol needs to be distributed among all the nodes as there is no central controlling unit. The nodes in MANET can leave the network and this should not affect the work of the protocol as the protocol works in any situation.

- Routing loop problem

The routing protocol should guarantee that the resources of the network are conserved like bandwidth and nodes internal resources link processing power, memory and battery. One of the common problems in routing is the infinite loop formation, this could occur if node (X) connects to any other node (Z) through an intermediate node (Y). X sends routing request to Y seeking for Z node, Y in turn thinks that the path to Z goes through node X and sends back a route request to X; this situation will cause nodes X and Y to keep sending to each other infinitely. The reason behind this behavior is that the link between Y and Z has broken and Y does not inform X for that failure and hence an infinite loop will be formed, consuming the network and nodes resources. Figure2.2 describes an example of such condition.

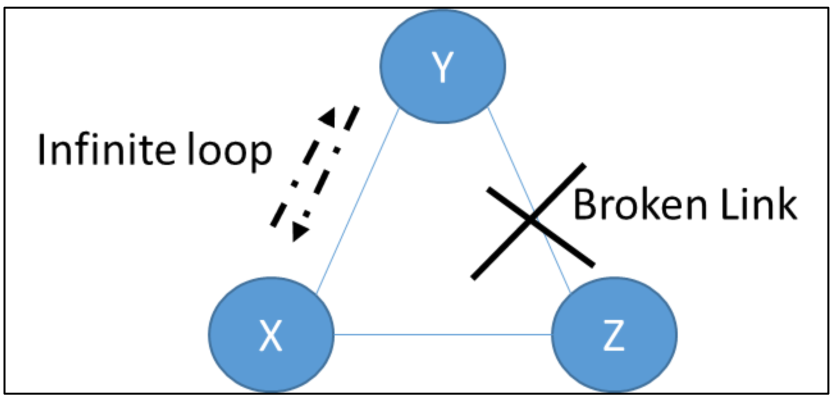


Figure 2. 2: Routing Loop Problem

The design of the routing protocol should guarantee to solve such scenarios to conserve the resources of the network.

- counting to infinity problem

The counting to infinity phenomenon occurs when members of MANET keeps incrementing each other hop count continually in loop. Figure 2.3 below shows a standard MANET consisting of four nodes (A, B, C and D). Consider that the link between C and D is broken, and A does not informed that C does not have a valid link to D. A before the link between C and D became broken stores that the way to D is through C with a hop count of 2. C in turn knows that the link to D is broken and removes that route entry from its routing table, Node

B also knows that the link is broken and deletes the entry from its routing table, B still knows that the link to node D can be achieved using node A with hop count equals 3. Node C acknowledged that node B has a valid route to C using 3 hops, the C will register that the way to D is through B using 4 hops. A receives that node C can reach node D via 4 hops, then A will update the route entry to D using C by 5 hops. That situation causes the nodes to increment each other hop counts to infinity.

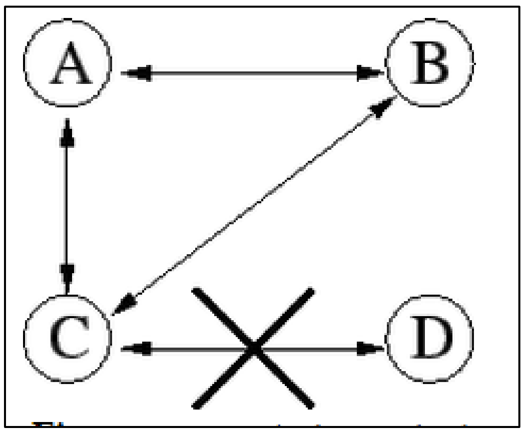


Figure 2. 3: Counting to Infinity Problem

- *Multiple routes*

Several routes may be formed for a specific destination, this is caused because of the routing table building process. This property gives MANET the necessary flexibility to route even in the presence failures of some routes in the routing table because of nodes mobility.

- *Control messages and overhead*

MANET requires a lot of control message exchange because the nature of the network. The nodes needs to be aware of each other and maintain routes as immediate as possible to guarantee the reliability of the network and reduces the delay in the route build process.

- Link state vs. distance vector routing

The conventional networks works in two forms in finding the routes within a network. Mobile ad hoc networks uses those conventional strategies with some modifications to commensurate with the special needs and nature of MANET.

The first method is link state routing [7], the basic idea in link state routing that the nodes in the network builds up a full view map of the entire network in a form of graph represents the nodes and all connections and links between nodes. Every node separately stores the best route for every reachable destination and keeps the gathered information in its own routing table. The nodes mainly keeps up only the paths with the shortest link cost. The link cost for each node is distributed in broadcasting technique, the nodes in the network update their tables based on the information about links costs obtained from the broadcasted messages in the network. Links costs may change during time because for example the long propagation delays of wireless mediums. Those information are updated periodically and hence updating the links states and routing tables.

The other class of routing is distance vector routing [7] [8]. The key idea in distance vector is every node maintains the distance to other destinations in network via its neighbors. The routing table of nodes in the network holds the destination of node and the number of hops and next hop node (neighbor) that leads to the concerned destination. Routing table is broadcasted periodically to the entire network every node receives the message will update the routing table based on these information gathered, and only maintain the entries with the shortest path in term of least number of hops. Figure 2.4 shows an example explains the process of building up routing table.

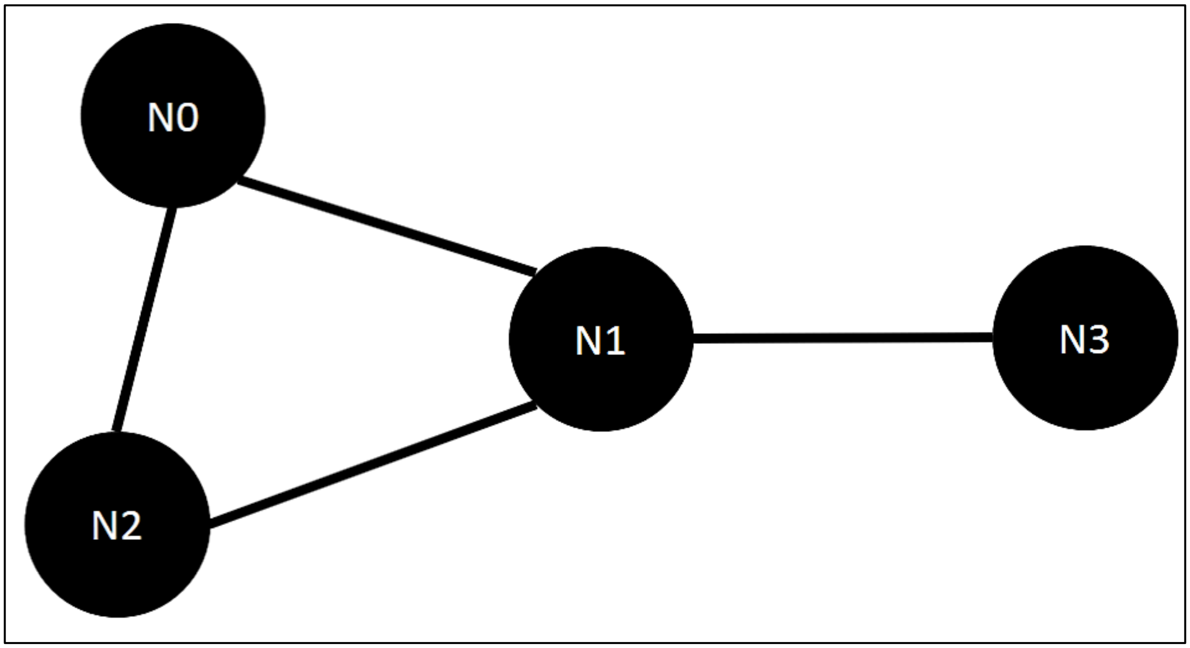


Figure 2. 4: Example of Distance Vector Route Calculation

Node N0 receives routing tables from its neighbors (N1, N2), the entries comes from N1 for N3 destination is (N3, 1, N3) – it means that for the destination N3 the number of hops is 1 and the next hop is N3 – and also for destination node N2 the entry will be (N2, 1, N2). The routing table form N2 will contain the following: for destination N1 it will be (N1, 1, N1) and for destination N3 it will be (N3, 2, N1).

Table 2. 1: Final Routing Table for Node N0

Destination	Number of hops	Next Hop
N1	1	N1
N2	1	N2
N3	2	N1

Node N0 after receiving routing tables from its neighbors (N1, N2), it will calculate the shortest path to all available destinations. The final routing table is shown table 2.1.

The basic metric in distance vector is the number of hops, the information in the routing table updated based on that metric. For MANET this metric is important in finding the shortest path available, but in some scenarios this metric is not enough to deal with this kind of networks and some modifications and enhancements are required.

2.1.4 Challenges with mobile ad hoc network

1- Dynamic Topology: the mobility of nodes in MANET causes the network to dynamically changing upon time and this feature requires the protocol to be aware of this rapid and inconsistence change of the physical graph of the network

2- Power: MANET is a group of battery powered devices like smart phones, laptops, and PDAs, etc. Those devices are limited in power and hence some kind of power conservation is needed.

3- Network resources: in addition to power, nodes in such networks have limited resources like bandwidth, processing power and also memory and storage. The protocols should not consume all resources to keep the network connected all the time.

4- Security: MANET works over wireless environment, and vulnerable to impersonate attacks. Authentication and encryption is needed to ensure some sort of security levels.

5- Heterogeneous nodes: MANET may include several types of hosts that work in different platforms. The protocol needs to be aware of this heterogeneity and capable of working in a complete integral form.

6- Communication links: symmetric and asymmetric links could be formed in MANET. The unidirectional links may exist because of the nodes mobility and the wireless environment of the network.

7- Interface to other networks: MANET could interact with other networks and uses its services like the ability to connect to the internet. This give a big problem when designing the routing protocol, the need for a protocol that is capable to deal with the internetwork and provides the required interface for the other networks.

2.1.5 Routing Protocols Classifications

Different protocols have been designed for MANET. Those protocols could be classified based on the network structure and routing strategy [9] [10]. Figure 2.5 shows protocols classification, the first is flat, the second is the hierarchal structure, and finally the geographical positioning protocols.

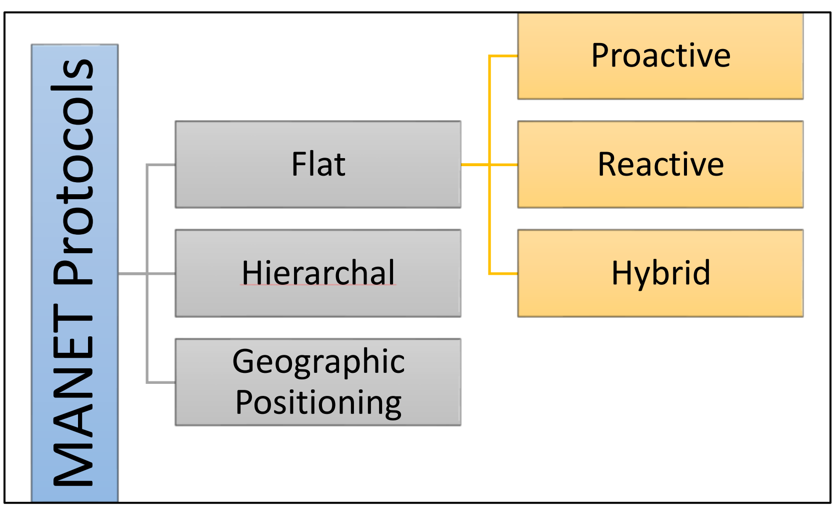


Figure 2. 5: MANET Routing Protocol Classification

The first group is flat routing [10] which is divided into three categories: proactive, or table-driven which requires the nodes in the network to maintain a full view of the entire network in a proactive way, i.e. to periodically flooding a route discovery messages in network and update the routing tables using the received messages. The other type is the reactive protocol, which only maintains paths upon request. Any node in the network and before starting to transmit data packets, it should first initiate a route discovery to maintain the route for the targeted destination. A third form of flat protocols is the hybrid protocols which uses both proactive and reactive techniques.

The second class is the hierarchal approach, which is used in high density approach to reduce the network overhead. Some approach is the clustering where the control of a set of nodes is coordinated by a cluster head how controls and leads the cluster members.

The third class of protocols is the geographic positioning approach [11]. The geographic positioning approaches depends on the physical coordinates of nodes obtained by GPS or even by a reference fixed point in the system. This approach is useful in reducing the total overhead of the network, this is because each node knows exactly where each node is situated and can forward messages to a direction in the network. This approach requires all nodes to know exactly the actual coordinates of each other which is sometimes not available, moreover the approach has to deal with high degree of mobility where nodes change their positions frequently.

2.2 Related Works

Our main work focuses on finding routes that has a high level of stability by estimating the link breakage time. Link breakage time could be estimated using several approaches proposed by several researchers, in the next lines we will mention these approaches and show the differences, advantages and disadvantages compared to our proposed model.

In addition, our model suggests using routes that has higher level of energy to prolong the network lifetime, other routing protocols uses power-aware routing approaches in different manners in hope to save the energy of the nodes participating in the routing process mainly.

In (MDA-AODV) [12] the authors proposes a new mechanism for finding routes with lower probability for link breakages to use as routing paths. The model suggests that the position and direction of movement calculated by using the GPS technology enabled at each node in the network, they also used the AODV routing protocol as the base protocol for their implementation. The process of finding the direction and speed of neighbor nodes occurs in the HELLO message phase procedure at each node when all nodes discovers their neighbors.

The information gathered (speed and direction) from the hello messages are stored in the Seen tables. The nodes that receives a RREQ message will forward that message only if its speed is less than a specific threshold, this threshold selected based on the density of network and maximum allowed speed of nodes. In the RREP phase, the destination node selects the previous hop based on its speed such that the speed of the previous hop is the lowest among all its neighbors rather than the minimum number of hops used in ordinary AODV. The RREP message will backward propagate until it reaches its final destination. The source node receives a route reply will use the received route information that registered in the routing tables of the intermediate nodes. This protocol prefers the routes with low mobility and hence the link breakages will decrease by excluding the nodes that moves away in high speed.

MDA-AODV shows good results in packet delivery fraction and overhead compared to ordinary AODV and many other performance metrics. However, the problem with such types of protocols that depends on the GPS technology suffers from degradation in network lifetime, as the GPS technology consumes a lot of energy, the proposed MDA-AODV can significantly decrease the entire network lifetime, as each node will consume significant amount of its energy in discovering the positions and mobility of its neighbors using GPS. The power is an important value in MANET routing and it needs to be used wisely. Moreover, in some situations devices may fail to use the GPS because it depends on pre-installed infrastructure (GPS satellites) and this infrastructure may not be available all the time especially in disaster and battlefields situations or even in normal situations inside buildings or in subways underground.

Other approaches in MANET routing is to use artificial Neural Networks to predict the mobility and locations of nodes in the network, NNs works based on machine learning algorithms. These prediction algorithms first used in WLANs as they work on the existence of pre-installed infrastructure like APs that can predict the mobility and motion of nodes and to which AP it will connect next. However, these classification algorithms still be possible to use in non-infrastructure networks, as there is a list of discrete locations. Several researches has shown that NN are the best choice to use when predicting the mobility of nodes like in [13] suggests.

The authors in [13] suggests using special prediction algorithm in a geographic routing protocol in ns-2 using artificial neural networks. This algorithm tries to find whether it is possible to use NN to get good results in predicting the mobility of nodes and aims to enhance the accuracy of the prediction process. The algorithm uses 7 inputs neurons that represent the current coordinates of nodes, timestamps, previous coordinates and timestamps, and 15 hidden neurons, 1 hidden layer and 2 output neurons that represent the predicted new locations of the node, also iRPROPR was used as a training algorithm. The algorithm applied inside the Greedy Perimeter Stateless Routing algorithm (GPSR) routing protocol. The algorithm used in GPSR protocol when the protocol needs to predict which node of its neighbors is closest to the destination.

The algorithm simply gives a previous coordinates as an input to a concerned node, this node will use NN to predict the new coordinates of its neighbors based on the input coordinates, and then the node selects the neighbor that has the shortest path to the destination based on the output predicted coordinates.

These types of approaches has several limitations, first is that Artificial Neural Networks is a black box, we does not know exactly what happens and how the output results are retrieved, because it depends on the hidden layers used by the algorithm. Moreover, the algorithm suggests that this algorithm needs to be applied by all nodes in the network to predict locations of neighbors and this requires extra processing power and energy.

Another important issue is that neural networks results are not necessarily accurate, it depends on several factors like the number of hidden layers used, and the learning algorithm and these inaccurate predictions may lead to un-desirable behavior of the routing protocol and could lead to misleading performance measures.

Other approaches for routing in MANET depends on the mobility of the nodes, and selecting the next hop depends on the speed, current position and direction of movement. An example of such schemes proposed in [14] where the authors suggested using the velocity-vector probability to find stable routes in the network, they used the AODV routing protocol as the base protocol, and they modified the algorithm in the route discovery phase in AODV. In the proposed work, the researchers suggested using two models in the mobility-ware probabilistic to find the routes with higher stability. The first is the Simple Velocity Aware Probabilistic (SVAP); the other is the Advanced Velocity Aware Probabilistic (AVAP). The proposed work classifies the nodes in the network into reliable nodes (RNs) that has a velocity similar to the sender and receiver nodes, and un-reliable nodes (U-RNs) which have velocity different from sender and receiver. The SVAP cuts off the U-RN by selecting only RN to rebroadcast the messages and building up routes. In the AVAP the researchers suggests using a probabilistic timer and function to differentiate between RN and U-RN, this helps in avoiding the simultaneous broadcast of nodes and the network and saves the network wireless medium. This algorithm shows better results rather than other probabilistic broadcasting schemes in terms of link breakages and stability of routes depending on the velocity vector of mobile nodes.

These types of probabilistic approaches depends on the information provided by each node, the problem happens when any node wants to gather information about the entire network or information about the one-hop distant nodes. The information exchange between nodes could lead to higher overhead in the wireless medium. Moreover, the energy consumption metric needs to be considered as MANET clients' needs to save its power as long as possible.

Some other approaches aims to select and use higher residual energy and higher link stability routes like in [15]. The authors suggested a new mechanism to select routes with minimum link breakage probability and higher residual energy of intermediate nodes and delay forwarding according to nodes degree of busy. This technique depends on the connection status of the links between nodes and a threshold is set based on the network density, this threshold used as a limit to identify stable routes among available routes in the network. The authors suggests using the VON program to categorize nodes into high-speed nodes and low-speed nodes and the communication load. In addition, the residual energy of the node is calculated and used to calculate the stability and reliability of the selected routes. The problem with such technique is that it uses a timer on the destination node. This timer used to wait for a specific period until the node can respond or forward the RREQ message to make sure that all RREQ messages received from all available routes, and then the target node will calculate the optimal route with higher degree of stability. This timer can delay the transmission process and causes undesirable performance in terms of delay. Moreover, the discovery of neighboring nodes speed is a challenging task because it could lead to undesirable overhead in the network and simultaneous broadcasting problem. Speed of nodes is a good indicator of link stability between nodes but it is not enough, the direction of movement also an important factor as the nodes that moves in higher speed and getting closer to the concerned nodes is better to use than a slow speed node moving away from the concerned node.

Other approaches depends on the quality of service awareness and link quality between nodes. This scheme proposed in Link Quality and MAC-Overhead aware Predictive

Preemptive AOMDV (LO-PPAOMDV) [16]. This protocol works based on the MAC layer overhead and link quality between neighbor nodes. The weighting formula combines both MAC overhead and link quality to find the optimal route between source and destination. The link stability measured using the transmitted signal power that is equivalent to the link quality metric. Moreover, nodes receiving any RREQ will also calculate the MAC overhead by estimating the channel occupational time in the link between neighboring nodes. The protocol also applies a congestion control mechanism to avoid high MAC layer overhead. The mechanism uses a “Route Failure Prediction Technique” based on the Lagrange interpolation for estimating whether an active link is about to fail or will fail.

This protocol works fine and shows good results in terms of overhead and less MAC and route errors. The problem with this technique that it suggests that the transmission power gives an indication about the link quality, however, in some situations where nodes are not moving but situated in the farthest edge of the transmission range of node. In this scenario, the link quality will be low as the node gets lower receiving power indicator but actually, the link is much more stable than another node moving in a high speed near the concerned node. In our model, we used the speed and direction of movement to estimate the link stability and link breakage time. Moreover, the distance between nodes is unknown and hence we need a mechanism to calculate the sending power metric.

Another approach uses cognitive agent to predict the resources based on the traffic and mobility of nodes in the network like in [17]. This protocol predicts the availability of access medium based on the mobility of nodes to enhance the performance in terms of delay and fair distribution of resources like power, buffer space, bandwidth and CPU among all nodes.

The Cognitive Agent (CA) uses BDI model and WNN on behalf of human intervention, this CA software designed by defining various models such as traffic, mobility, buffer, energy prediction and bandwidth prediction and the interaction among these models. The mobility model assumes that each node knows exactly the current location in (x,y) dimensions, these locations are sent to all neighbors of the concerned node, then the node uses WNN to estimate the new locations of that node. The estimated mobility and traffic predictions used to control the resources of the network.

The protocol proposed depends on using Neural Networks to predict the new N locations, speed of each mobile node. This method has a high degree of successful estimations, but the problem with this method is that it suggests that each node is able to retrieve its location and speed and broadcast this information to all its neighbors. However, the nodes in MANET are limited and lacks the techniques that can provide location and speed; the speed calculated in relative to each other not the absolute geographic position and speed. Moreover, the direction of movement ignored. In our proposed model, the speed and direction of movement considered relatively to each other. Another problem with this model is the processing power needed to accomplish all these calculation to estimate mobility and traffic, these issues needs to be considered.

Our model is an enhancement and extension of our previous work in [18] [50], we proposed a new model for estimating the link breakage time between source and destination based on three parameters: mobility, residual power, and node’s local resources. We suggested using a weighting algorithm to balance the load of the routing load among nodes that has higher residual energy and higher local processing power, also we focus on selecting routes that has higher level of stability and expected to last for a longer time. As a result, the occurrence of link breakages expected to be lower. To estimate the link breakage time between two neighbor nodes we predict the time that the two clients will remain within the transmission range of each other. To do so, we used the Received Signal Strength Indicator (RSSI) to measure the distance, speed and direction of movement whether they move closer to each other or moving away from each other. Based on the information collected (distance, speed and direction of movement) we can predict the time that the nodes will remain reachable by each other and hence the link duration period.

The residual energy of nodes metric helps on increasing the total network lifetime and saves the nodes energy for further tasks. Our algorithm uses the residual energy of each node wisely and selects routes that has intermediate nodes with larger residual energy levels. Moreover, we select nodes that has higher processing power; the nodes with larger capabilities can hold up the heavy duty in the network and saves the energy of low-specifications nodes.

2.3 contributions

The dynamic topology in MANET exposes the network to many problems; one of these problems is the number of control messages needed to accommodate these changes in the network. The major problem occurs during the transmission of data packets from source to destination, many intermediate nodes loses its connection, hence a link failure occurs, and new routing request re-triggered. To solve this problem, the routing protocol should use routes from source to destination with higher stability (i.e. lasts for longer time). However, in MANET networks, the nodes moves randomly and in different speeds and directions, and there is a need to predict its mobility behavior before using these nodes as an intermediate nodes to bypass messages to destination. As we noticed in the previous works, several approaches exists to estimate the mobility behavior of nodes. Most of these approaches depends on three major techniques, (1) using geographic positioning systems like GPS technology, (2) using artificial intelligence techniques like neural networks and (3) using received power indicator. The problem with using geographic information that it consumes a lot of energy and needs high capable devices to run and not all wireless-enabled devices has these specifications. The second technique uses neural networks algorithms to predict the mobility and these algorithms needs a lot of processing power and energy from the clients which is not available in MANET clients, moreover, these techniques has a high level of unsuccessful predictions which can results in very bad performance for the routing protocol. The last technique uses received power as a metric in estimation distance between nodes.

In our proposed model, we aim to estimate the link breakage time between all nodes within any available route from source to destination, the proposed model selects the routes that has higher stability value based on the estimated time that the link will remain active. The model utilizes several RSSI signals to measure the average distance and speed of mobile node within the transmission range of another node. The final estimated link breakage time is the minimum estimated link breakage between all pairs of one-hop distant nodes within a candidate route. In addition, to save the power of nodes in the network and prolong the network lifetime we added the residual energy metric. The proposed model prefers nodes with higher energy value to use as an intermediate node within any candidate route. The residual energy metric is the total cumulative energy of all intermediate nodes within that concerned route. By combining out these two metrics we can reach a higher stable and long living routes that will potentially enhance the network overall performance.

Chapter 3: Mobile ad hoc network Routing Protocols

3.1 Ad hoc on demand distance vector protocol:

3.1.1 Description:

Ad hoc on demand distance vector protocol (AODV) [19] [20] is one of the most effective and adaptive routing protocol for MANET networks. It is a reactive protocol where routes only established upon request; moreover, AODV uses distance vector algorithms for route calculation with the difference that only nodes that receives route request only participate in the routing process and nodes that does not receive these control messages does not participate and does not update its routing information. In addition, clients that uses AODV protocol does not maintain any routing information and their routing tables stay static and does not change until these clients' needs to send or receive data.

Ad hoc on demand distance vector protocol uses route-discovery mechanism [21], with the difference that nodes in AODV builds routes tables dynamically and upon request, this difference will reduce the network overhead, as no periodic route and control messages be exchanged. AODV uses local discovery broadcast messages for each node to discover out its neighbors only (not the entire network), this "hello" messages gives the benefit of making nodes aware of its neighbors and the process of establishing new routes takes less time as each node is aware of local changes of its neighbors. AODV uses sequence numbers presented in DSDV [22]; any node in the network maintains a new incrementally increased sequence number, these incremented sequence numbers are used to replace old invalid routes.

3.1.2 Route Establishment:

The process of routing starts when a source node initiates a route request message (RREQ) and broadcasts this message in the network searching for a targeted destination. RREQ message holds the address and a sequence number of the source, broadcast ID, destination address, destination sequence number, and hop counter. For each node receives route request message first it determines if it is the target destination then it will reply with route reply message (RREP), and if it is not the desired one it will rebroadcast the message to its neighbors and increase the hop count field with one. In order to build the reverse route from the target node, the intermediate node will track some information about the route.

Building up the route also depends on the entries in the routing table in the node that receives a RREQ; the node decides if the route exists and new by its sequence number, if so, it will respond by a RREP that it has a valid route to the destination; otherwise, it will rebroadcast the RREQ to its neighbors. During this process, a reverse path setup is built. The reverse path route depends on the sequence number of source and destination in addition to broadcast ID to specify how fresh of the request is. Each node receives a request from a neighbor it will record the address of that neighbor to send it the route reply message. Finally, the node that receives several RREPs for the same route, it will select the most up-to-date one and with the least hop count number.

When RREP received by the source node it will record the path and start sending data. When multiple routes received, the source node will select the route with the minimum number of hops.

3.1.3 Route maintenance:

A route failure may occurs when intermediate node finds that a neighbor that it uses to forward messages to the destination is no longer valid. The node will remove that entry from routing table and sends a route failure message to its neighbors uses that route (as it stores a list of the nodes uses that route) informing them that this route is invalid. All neighbors receives route failure message will also remove the route entry and forward the message to the neighbors of interest. The failure message will also reach the source; the source will send another RREQ or will stop sending data.

3.1.4 Routing table information:

Each node routing table will keep the following fields about each destination of interest:

- Destination: the route destination (destination IP)
- Next Hop: the next node for that route entry
- Number of hops: nodes within that destination route
- Sequence number: the sequence number of that destination
- Active neighbors: a list of all neighbors uses this route
- Entry expiration time: For each route in the table, a validation timer is set to keep its lifetime.

3.1.5 Evaluation of AODV:

AODV uses distance vector routing technique with the advantage that AODV reduces network overhead, this is because AODV builds routes upon request from nodes, and no periodic route building messages used. In addition, AODV can react relatively in the presence of high degree of network topology change because of mobility.

Another advantage is that AODV uses sequence numbers to guarantee the how fresh the routes are, and solves the free loop problem [23], and solves the count to infinity problem, which is a typical problem in distance vector protocols [24]. In some cases, sequence numbers may fail and does not provide the required task, this could happen when partitioning the network or some nodes get out of the network during the synchronization process.

Overhead goes larger as the network size becomes bigger, in the case of big size network, AODV may show several drawbacks. Overhead increases significantly and link breakage will occur in a higher probability when going throw big number of hops and when going for longer distances, also; what will happen when transferring bigger amount of data from source to destination? Those problems needs more appropriate solutions.

AODV uses single route to a destination and choses the optimal one among available routes based on hop count metric. Once selecting a route, it will be stored as the only route for that destination. This requires that when some breakage occurs with that route, the source will regenerate another route using the RREQ message; which clearly increases network overhead. To solve this problem the protocol should store all the available routes to use them when needed.

3.2 Dynamic Source Routing Protocol (DSR)

3.2.1 Description:

DSR is one of the common reactive protocols in mobile ad hoc networks. It builds up its routes based on request from the sources to a specific destination. DSR on the contrary of AODV protocol does not depend on a routing table; it uses a dynamic source routing to discover the route to the target. [25][26]

DSR uses on demand route-discovery mechanism and route-maintenance to handle requests of different nodes. Where the route discovery uses source routing mechanism where the RREQ message from the source holds the complete ordered list of the nodes in the route from the source to destination.

3.2.2 Routing Mechanism:

The process of routing first begins when a node wish to send data to a specific target node, it first broadcast route request message to all neighbors and start listening for a route replay message. Every node receives a RREQ will check its route caches for a valid path to that target node, if no routes found to that destination, the node will also broadcasts that message to its neighbors after adding its address to the message. The message propagates until it reaches its final target or reaches a client that has a valid path to the final target.

To initialize the route caches of the neighboring nodes the source sends a RREQ message that has a hop count limit set to zero to prevent the neighboring nodes from forwarding the message. Another useful technique that DSR make use of is to overhear all the packets that the node receives this allows the node to scan the information in the packets and make use of the useful routing data in the received packets then the packets will be discarded.

A RREP message is sent from the target node or from the node that holds a valid route to the destination using the reverse order of the addresses in the RREQ message. Another way for routing back is to use the RREQ targeted at the originator to find the correct path, this requires to store the route in the routing cache with time stamp and to use the routing maintenance mechanism to build up the route.

When a route has a failure because an intermediate node is lost or turned off, this could be discovered by overhearing for acknowledgments or a node may overhear its neighbors for packets forwarding. When such failure is detected an error message is sent back to the source and the node caused the error is removed from the routing cache, also all routes containing that node will also be truncated.

3.2.3 DSR evaluation:

DSR has several advantages and disadvantages compared to other protocols:

By studying out DSR protocol we notice a significant advantage of DSR; it make use of the information provided by routing process between a source and destination, that is; the intermediate nodes will get information about the routes to other nodes that uses the same route request message and will store those routes in its routing cache which as overall will reduce the network overhead. Another advantage, DSR is a reactive protocol, no periodic messages are sent all over the network and hence reduces the network overhead, this also will lead to save the power of the mobile nodes as they don't need to receive or send periodic messages.

DSR protocol stores the intermediate nodes addresses while the RREQ message propagates throughout the network and this will lead to bigger and bigger messages especially in longer and high density networks. Another disadvantage, DSR may introduce further network overhead in the process of routing maintenance. Some security issues arise when DSR enables nodes to overhear every message in the network regarding of its contents, some sort of encryption is needed to achieve security.

3.3 Temporally ordered routing algorithm (TORA)

The basic idea in temporally ordered routing algorithm (TORA) [27] that it aims to minimize the protocol reaction in any topological change in the network because of nodes mobility and selfish behavior. TORA uses only small set of nodes to build out routes, this set of nodes only able to send the required control messages. Moreover, TORA uses three basic techniques to control the routing process: first is routing process, second is maintaining routes and the third is route erase. TORA algorithm is a based on type of algorithms called link reversal algorithms [28]. Link reversal algorithm is a distributed algorithm design technique which models out the problem into a directed graph and reverse out links in appropriately.

3.3.1 Routing Mechanism:

The process of building a route in TORA begins when a node wants to communicate with a target node. The route building phase begins and assigns directions for all links in the network or part of it, the route creation process builds up a directed cyclic graph rooted to the target. First, the source node broadcast a query message QRY, this message will propagate the network until it reaches the final destination. The target node will reply with an update message UPD to the clients that it receives the QRY message from. TORA aims to build up a hierarchal form of heights from source to destination. So when the target node receives the QRY message it will set a height value for itself and sends out UPD to the nodes it receives the message from. Each node receives the UPD message will in turn sets out a height value that is greater than the value in the received UPD height value. By this way a result of directed links to the originator of QRY are formed and also several routes are available.

To be aware of frequent topology change, the routes needs to be updated such that a finite time is set to validate the routes, this predefined time is used to set all available targets using targets graph of the network. During the detection of a network part, all links in the part of the network that has become divided from the target are flagged as undirected to delete wrong and out dated routes. The deletion of routes performed by clear messages.

3.3.2 TORA evaluation:

This protocol is highly adaptive in high dense networks, it can perfectly handle the fast topological change in the network and it prevents the nodes from clearing out all the routes in the network; i.e. it only work locally when failure occurs. The worst about TORA is the high overhead in the network because of the big number of control messages being transferred. Also TORA can produce multiple routes but actually only one route is available because TORA builds out the routes based on the height of the nodes which in turn depends on the number of hops to the destination.

3.4 Destination sequenced distance vector (DSDV)

Destination sequenced distance vector protocol (DSDV) [29] is proactive table-driven routing protocol for mobile ad-hoc networks. DSDV is like other distance vector protocols in the mechanism of routing, but DVDS guarantees loop freedom. This loop-free is maintained by using sequence numbers to guarantee the freshness of routes so that no loops will be formed within the network. DSDV is table driven routing protocol and hence it uses periodic updates to fill out the routing table.

Each node in the network should store all routes to reachable destinations, this basically possible by sending out periodic update from all neighbor nodes. Two types of updates are used: one is the periodic update after specific time, the other is trigger updates that are fired in between periodic updates and used when change in the routing table occurs.

3.4.1 Routing Mechanism:

Every node in the network should has information about the reachable destinations in the network and a routing table is stored in each node. The routing table contains three parameters: address, sequence number and hop count to that destination. Every specific period of time each node broadcasts its entire routing table to other nodes, this will result in up-to-date knowledge about the network. When a node wants to send data to another target node then it will directly look inside its routing table and start forwarding packets.

Updates are accepted and stored in the routing table if the sequence number of any route is greater than or equal to the old route, if 2 routes with same seq. number, the one with smaller hops is stored. Because of dynamic changes in the network, the nodes broadcast routing tables update to inform about these changes, or these updates are sent when detected. Initiating an update packet, the routing algorithm sets the hop count to 1 to indicate that the distance is one hop far.

The entries in every client routing table needs to be changed quickly and frequently to cube all the changes in the network topology, the changes primarily occur due to mobility and out of reach conditions. Up to date routing entries requires that each node to be aware of all changes in the topology, and acquire new information collected from the routing update broadcasts data upon link breaks or nodes failures periodically, this will make nodes locate and discover their neighborhood dynamically. The nodes can use these up to date information to deliver data packets upon request. [2]

DSDV can handle topological changes, when a node detects a change in the network topology or broken links the node will broadcast a message that holds new sequence number and sets hop counter for that broken link to infinity, and every node also will update their tables for that new information.

3.4.2 DSDV evaluation:

DSDV has the same properties as distance vector protocols and as a proactive protocol it keeps information about the entire network. This reduces the delay time needed as in the on-demand protocols where nodes needs to wait to find out routes before start to transmit data. Moreover, DSDV is loop-free protocol as it can prevents loop from being created during updating routing tables, the protocol uses the sequence numbers to make sure the route is up to date and fresh.

DSDV has several drawbacks, one is route fluctuation [2] which occurs because of its criteria of route update. Routes are preferred when their sequence number is newer or hop counter is smaller when sequence numbers are equal, and all other routes will be discarded or will not be preferred. This could result in a situation where some node receives an update and forward the update back and forth even no topological change has happened in the network.

Another problem with DSDV is the overhead of the control and update messages in the network as those messages needs to be sent periodically even when no change in the network topology occurred. Moreover, DSDV maintains routes that will never be used. Also, multi-path routes is not supported in DSDV as it only uses single route and discard all others.

3.5 Optimized link state routing protocol (OLSR)

OLSR (optimized link-state routing) [30] protocol is table-driven pro-active protocol, it uses link state schemes to retrieve information about all available links in the entire networks. Link-state routing approaches floods out the network with control and discovery messages to get the state of links in constant periods of time, this scheme will result in a high overhead in the network, especially when dealing with wireless mobile networks.

OLSR has the advantage of using the multipoint relays (Discussed below) to optimize the links being flooded in the network. OLSR uses tables to obtain routing information, those tables are built in a verity of control and update messages to handle out the network topological change.

3.5.1 Multipoint relays

Flooding the network with control messages increases the overhead, to reduce overhead, OLSR uses multipoint relays (MPR) [31] [32] technique. MPR can minimize the number of control messages needed to discover the network, it depends on a set of neighbor clients as a multi-point relays for a specific node, only multipoint relays of one node forward control messages comes from that node. Figure 2.6 below shows multipoint relays of a specific node N. The nodes in grey are the MPRs for the node N.

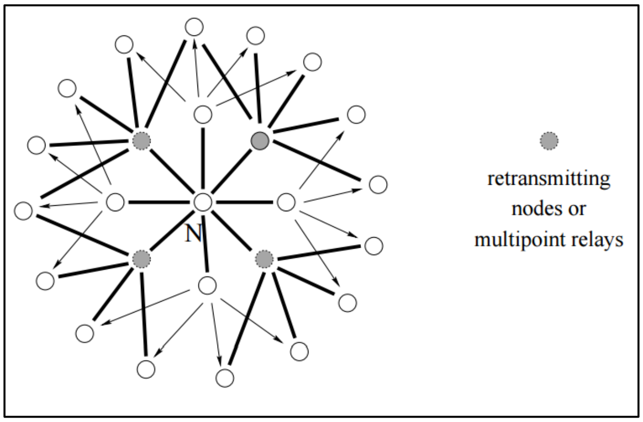


Figure 3. 1: Multi-point Rely of node N

3.5.2 Routing mechanism and control messages

Routing in OLSR uses three different control messages (HELLO, TC, MID). The first process is to detect the neighbors, each node in the network sends out should detect all the surrounding one hop nodes, and this is done by sending out HELLO messages periodically to sense out neighbors. The HELLO messages contains information about all one hop neighbors and also the link status whether it is unidirectional or bidirectional links, also the link could be either multipoint relay if this node is selected as a multipoint relay or even lost if the link is broken. Those messages are sent upon constant period of time. By this method each node in the network has information about all 2-hop nodes distance, those information also kept in the nodes for a specific period of time.

The basic idea behind selecting the MPR is to first find all the one hop reachable neighbors, these 1-hop far set will form the MPRs for a specific node, these neighbor nodes will also cover all their 1-hop distant neighbors and as a result the concerned node has MPRs that reaches the 2-hop distant nodes, i.e., the MPRs and their 1-hop distant neighbors forms a 2-hop distant set of the concerned node. The MPR calculation process is repeated every time a change in the 1-hop or 2-hop nodes has been observed either by losing a node or a new node is discovered. Moreover, every node in the network has “MPR-selector-set” which represents the group of all nodes that the node selected as its MPR nodes, the node only forward packets received from the MPR-selector-set.

Topological information retrieved at each node using TC (topology control) packets. These TC packets are broadcasted periodically by multi-point relays after every predefined interval time. The TC message declares all its MPR selector set. The TC message is flooded in the network and take advantage of MPR technique to reduce the overhead of control messages. Any node can reach all nodes using MPRs or directly. Those topology information are kept for TOP_HOLD_TIME period until they are considered invalid.

The information collected about topology and neighbors are used to forward messages from source to destinations immediately and the information are refreshed periodically. The path to be used from source to destination is based on a selection algorithm based on the shortest path calculation; OLSR uses Dijkstra's shortest path algorithm [33]. The optimal path is the rout that has the minimum number of hops to a specific destination.

3.5.3 OLSR evaluation

OLSR protocol is like other proactive protocols where no delay when a client decides to transfer data to other destination node, it also does not need any administrative central management and can handle the entire network independently. Control messages in OLSR are sent every specific period of time and does not need to be delivered in sequence. OLSR is suitable for situations where the delay is not acceptable and quick delivery is needed.

The big disadvantage in OLSR that it needs more time to detect a broken link and depends on the discovery interval times suggested by OLSR [34]. Moreover, OLSR needs higher processing capabilities when attempting alternative routes.

3.6 Dynamic MANET on-demand routing protocol (DYMO)

The DYMO protocol [35] [36] is a successor of the Ad hoc On Demand Vector protocol and it can work as proactive and reactive protocol, the protocol is defined in the IETF internet-draft in its sixth revision and still working on it. DYMO works simply as AODV in its operations mode, it differs that it is simpler than conventional AODV protocol. As the other on-demand protocols it first sends a route request packet and then when route reply arrives it can send out data to the desired destination. The protocol has another operation which is the route maintenance that is used when error occurs while transmitting data. The routing table consists of several fields as shown in the following table 2.2:

Table 3. 1: DYMO Routing Table

Destination Address	Sequence Number	Hop Count	Next Hop Address	Next Hop Interface	Is Gateway	Prefix	Valid Timeout	Delete Timeout

3.6.1 Routing mechanism:

When a node S needs to send data to another node D it first generates and sends a route request message (RREQ). Also the sequence number obtained by the node also incremented in the RREQ message and broadcasted for all the neighbors. Figure 2.7 [37] illustrates the process, when node 2 wants to communicate with node 9 it will send out a route request message holding the origin address which is 2 in the example and also the destination 9, also the sequence number is included in the message after being incremented, all nodes receives this message (1, 3, 4) will forward it to all its neighbors holding out the previous source destination information adding the forwarding node address which is needed for the reverse route building.

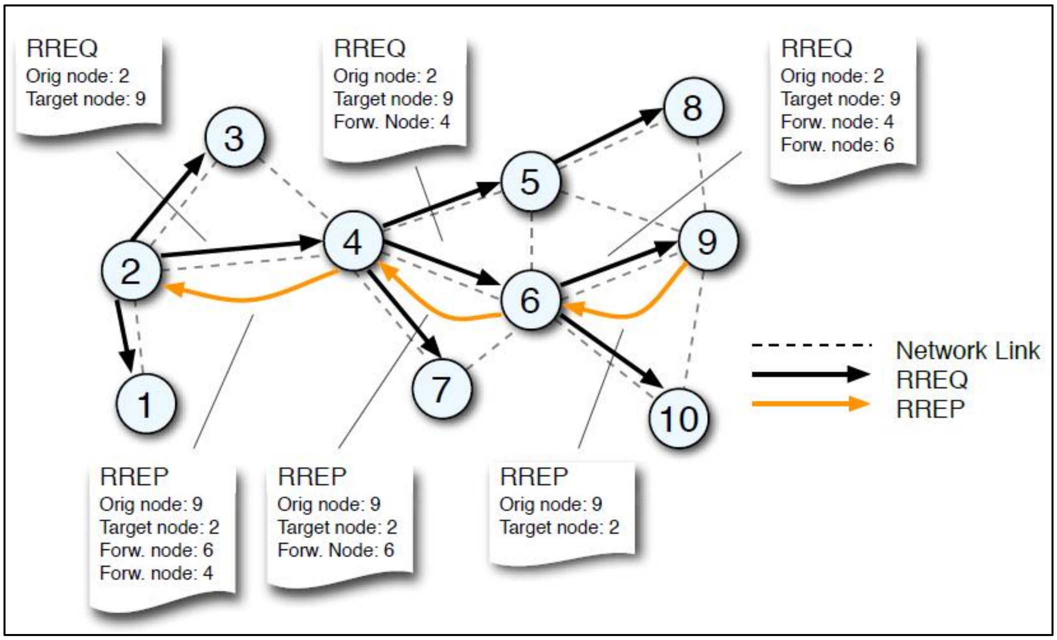


Figure 3. 2: Example of DYMO Routing Process

The message will propagate throughout the network until it reaches the destination node (9). The destination node will reply with RREP message to the source of the RREQ using the reverse order of the forwarding nodes.

A special characteristic in DYMO that if the source node knows the sequence number and the hop count of the destination it will include it in the message as this will help the intermediate nodes. The forwarding nodes append the address and sequence number of its own and also the prefix information, gateway information to the route request message. The source node will wait for a specific period, if no RREP arrived it will try again.

As shown in the figure above; the destination node (9) will reply using the original path that it receives the RREQ message from, this means that DYMO does not support symmetric links, it only works using a bidirectional support networks.

When failure occurs during the transmission process between source and destination, this situation occurs when a change in the topology occurs when a node receives a packet concerning a specific route, and that route has become invalid. Valid timeout field in the routing table holds out the validity time for every entry in the routing table. When the forwarding client receives a message for a node that it does not have a routing entry, it will reply with route error RERR message to the originator of the packet using the reverse path appended. Moreover, the node creates the RERR message also include all the entries concerning the unreachable node as next hop node. By this way the node will notify all nodes about the routes that are no longer available, the message is broadcasted throughout the network.

3.6.2 DYMO evaluation

The DYMO protocol is on-demand protocol which means it is more aware of topological changes and also has the advantage of reducing the overall overhead in the network. Moreover, DYMO get benefit of the information provided by RREQ messages to get a view of all available routes concerning a specific destination. In addition, the RERR gives another advantage in giving information about broken and invalid links in the network. The DYMO is better than AODV that it performs well in high mobility environment as it rapidly get information about topological changes.

The major con of the DYMO is that it shows great overhead and unnecessary control messages exchange in low mobility scenarios.

In chapter 5 next, we will study four of the previous discussed protocols and evaluate the performance of these four protocols under extreme conditions of mobility and limited power sources. These four protocols are AODV, DSR, DSDV and OLSR. We selected these protocols exactly because these protocols are still be used although they are a little bit old. According to several studies [51] – [54], these four routing protocols shows the best performance and the optimal solutions for MANET routing, the other reason is that these protocols are well-implemented and has higher degree of robustness on the programming level and algorithms used. The most important factor that make us use such protocols in our study is the problems we discussed in the background in chapter 2, the counting to infinity problem and the free loop problem are first solved using a robust and efficient approach using sequence number which is used by these protocols. So using such protocols in MANET routing solves a lot of problems in MANET which until now no other routing protocol achieved. The other recent approaches discussed in the related works section in chapter 2 are also used one of these four protocols to build up their approaches because of the reasons we mentioned.

Chapter 4: Simulation Setup

4.1 The network simulator (NS-2.35)

NS-2 [41] is an object-oriented simulation environment that uses tool command language "TCL" scripts to build network scenarios and simulations. NS-2 works under discrete events targeted at networking scenarios. NS-2 is built using C++ and an object oriented tool command language (OTCL). Network Simulator 2 provides a supportive environment for wired and wireless networks and supports TCP, multicast and routing protocols. The basic structure and simulation flow for NS-2 is show in figure 4.1 below:

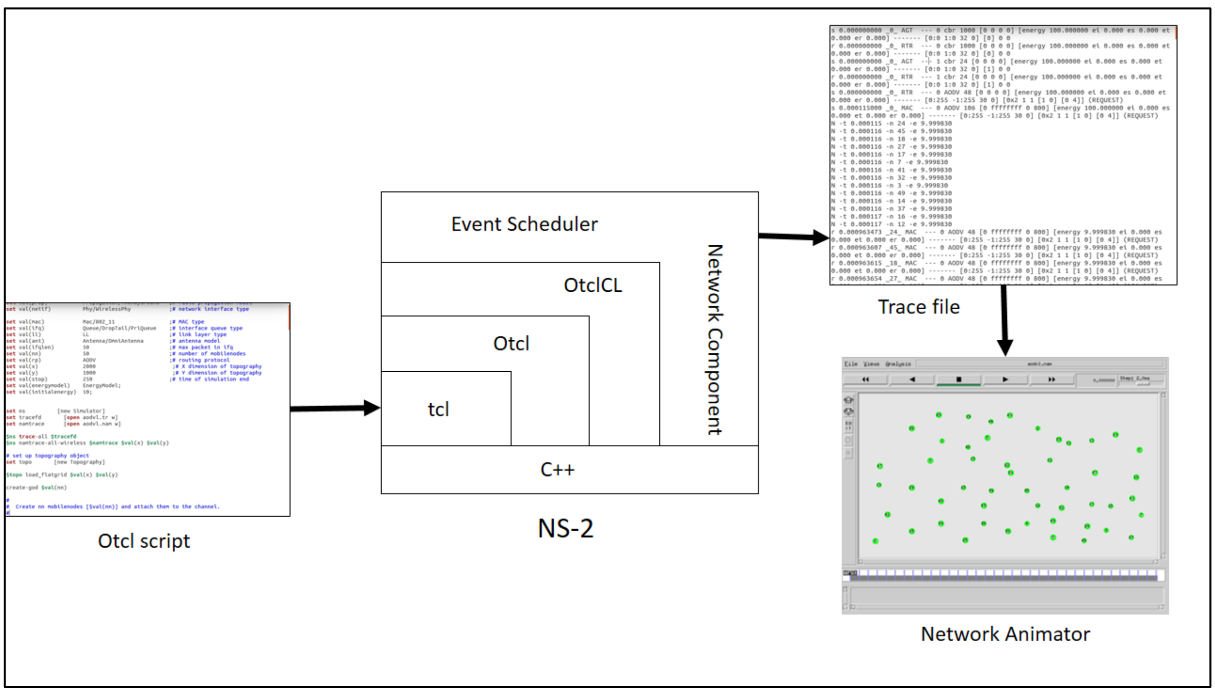


Figure 4. 1: NS-2 simulation flow

NS-2 is built using C++ language, the user provides an Otcl scripts and the NS-2 interpreter converts the Otcl code into c++, the Otcl script includes the nodes configurations, links, and also the flow and connections, and of course the protocols used. The resulted output is a trace file that contains all the resulted events that occurred in the simulation. The trace file is used to calculate the results like throughput, delivery ratio, etc. NS-2 also has a network animator (NAM) plotter that visualize the network. NAM reads the trace file and visualizes the events in the simulation like mobility and packets that propagates throughout the topology.

NS-2 provides a sustainable environment for ad-hoc networking and provides all the needed routing protocols implementations, also contains the necessary mobility and power extensions for our simulations. We used the most recent version of NS (version 2.35) released in 2011.

4.1.1 Mobility model

The mobility approach we implemented in our simulations is based on the CMU monarch project [42] that is embedded in ns-2. The mobility of nodes within a predefined topography enables the nodes to change their positions and velocity during the simulation time. The movement of nodes occurs based on a predefined pattern that specifies the mobility of each node. We applied this model in our simulations

4.1.2 Power model

The power model implemented in ns2 enables the nodes in the network to decrease its power according to different modes and activities. In NS-2 the power consumption model can be set by user and the modes that causes the node to lose some power is in the transmission mode, receive mode, sleep mode, and idle mode.

In real life, devices losses its power due to different several factors, the amount of power consumed depends mainly on three factors: (1) the size of the packet (received or transmitted), (2) channel bandwidth, and (3) network interface card specifications. When any node wants to transmit a packet it will consume the following:

$$\text{Energy}_{\text{tx}} = (\text{transmission power} * \text{Packet size}) / \text{bandwidth} \quad (1)$$

For example to transmit a packet of size 512 bit with transmission power of 1.0 W over a channel with bandwidth of 2Mb, the amount of energy consumed equals 1*512/2*10^6 joules. Also, some of the power is consumed to NS propagation model, the wireless propagation model is set to transmit the signal up to 250m range this requires a 0.2818 W power to accomplish [43]. The total power consumed for any specific node at any specific time is shown in equation 2 below.

$$E(t) = P_{tx} * T_{tx} + P_{rx} * T_{rx} + P_{sleep} * T_{sleep} + P_{idle} * T_{idle} \qquad (2)$$

Where:

P_{tx}: power at transmission mode.

P_{rx}: power at receive mode.

P_{sleep}: power at sleep mode.

P_{idle}: Power at idle mode.

T: is the time spent at each mode.

In our simulations, the power at each mode is user defined as different network interfaces uses different power values, and we only want to evaluate the routing protocol behavior and how it affects the power consumption at individual nodes level and on the overall network lifetime.

4.2 Simulation environment:

The simulation environment represents all the factors that plays roles in determining the efficiency and performance of routing protocols in MANET, the routing protocol is affected by one of several simulation environmental conditions which include: the traffic type and load, size of the network, mobility of the nodes, and power conservation. We will explain each of those parameters:

4.2.1 Traffic (type and load)

The traffic type is the type of the data being transferred from sources to destinations, NS-2 provides two types of flows types, the first is the constant bit rate flow (CBR), and the other is the transmission control protocol (TCP). In our simulations we used the CBR flow over UPD connection, we did not use the TCP because the TCP protocol has undesired features like retransmission and flow control [44], we only want to evaluate the protocol behavior and not the flow, when comparing routing protocols, the time for sending the packet will be different in the case of TCP, therefore it is difficult to compare protocols in the presence of TCP flows.

The network traffic load represents the amount of data being transferred within the network, this include the size of the load and the number of packets generated and sent per unit of time, for example some simulations we choose the data packet size to be 512 byte and the sending node will generate 5 packets per second, this means that each individual source will generate 512 * 5 byte/second for each individual traffic flow, this load will be either delivered to the destination or will be dropped due to many reasons, our purpose is to measure how much of that load is transferred successfully to the destination and how long it will take to deliver that load, the results depends on the routing protocol behavior that we will evaluate.

The entire network load also depends on the number of destinations, in other words, the number of flows being generated in the network, for example, in some simulations we set the number to 10 CBR flows, which means, 10 source nodes will send data to other 10 destination nodes. Again, the number of flows will affect the protocol behavior which we are interested in measuring. Some of the protocols may show lower performance than others when we use the same amount of load for all simulated routing protocols.

4.2.2 Size of the network

The size of the network represents the number of active nodes that do participate in the network, in NS-2 we used constant number of nodes for most simulation runs, we only want to evaluate the protocols behavior under the same number of nodes for all tested routing protocols, the network topology also includes the area dimensions where nodes moves around, these dimensions (Width X Length) represents the area where nodes can move in the (x, y) dimensions. Note that NS-2 also includes the third dimension (z) which represents the height, we don't include the third dimension in our simulations because our work only valid for flat topologies where all nodes are on the same level, a third dimension will not affect the performance of any protocol, we use wireless channels as a medium for communication, hence, no difference whether the nodes are in three dimensions or two, because the only factor that matters is the absolute distance between each pair of nodes. At the beginning of the simulation, each node should have an initial position within a predefined topology region, for example, in a topology of (1000m X 500m), we can set the initial position of any node within the interval [0-1000] in the X dimension, and in the interval [0-500] in the Y dimension.

4.2.3 Nodes speed and mobility

Mobility of nodes in the network is a very important parameter that influence the performance of the entire network, we can define the mobility factor of the network as the speed at which each node moves within the topology area, in other words, each node in the network has an initial position in the network topology, the node could change its initial position to new coordinates at any given time during the simulation. Moreover, the moving node has a velocity, which represents the speed at which the node is moving toward its new position. Another factor that affects the mobility metric is the pause time. Pause time is the time that the nodes stop moving before it decides to move to another new position. For example, if we set the node to move randomly at a speed of 20m/s and a pause time for 5 seconds, then the node at the beginning will move to a random position a velocity of 20m/s, after it reaches its new position, it will wait for 5 seconds then it will decide to move to another new position at the same given speed. This process continues until the end of simulation time.

Mobility pattern could be built from scratch, i.e. the user can build his own pattern of movement, or could use one of the most popular patterns defined in [45]. Some of the most common mobility patterns are shown in table 4.1 below.

Table 4. 1: NS2 mobility models

Mobility Pattern	Application	Temporal Dependence	Spatial Dependence	Geographic Restriction
Random Waypoint Model	General	NO	NO	NO
Group Mobility Model	Battlefield	NO	YES	NO
Freeway Mobility Model	Metropolitan Traffic	YES	YES	YES
Manhattan Mobility Model	Metropolitan Traffic	YES	NO	YES

The first mobility pattern is the Random Way Point pattern, nodes in such pattern chooses a random new position and moves towards that new position using any speed between 0m/s up to “SPEED_MAX”, max speed is user defined and used to restrict the velocity of the node. The node also uses pause time, after it stops in its new coordinates it waits for a period of “PAUSE_TIME” seconds before it moves to another new position with another new speed within the interval [0-speed max]. Figure 4.2 below shows the Random Way Point pattern.

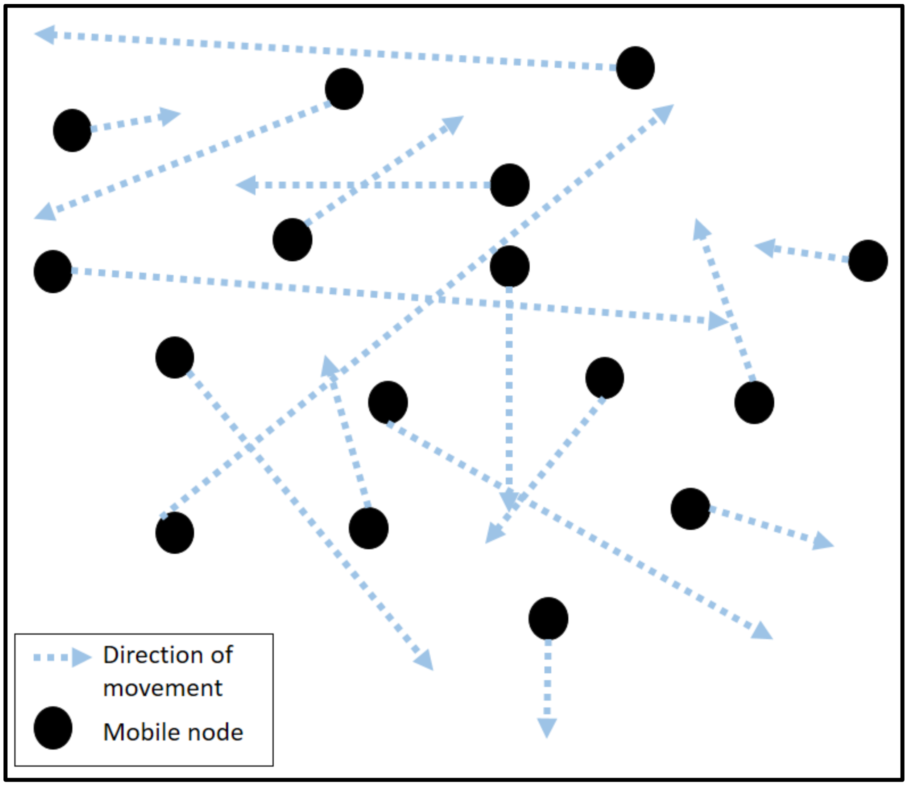


Figure 4. 2: Random waypoint mobility model

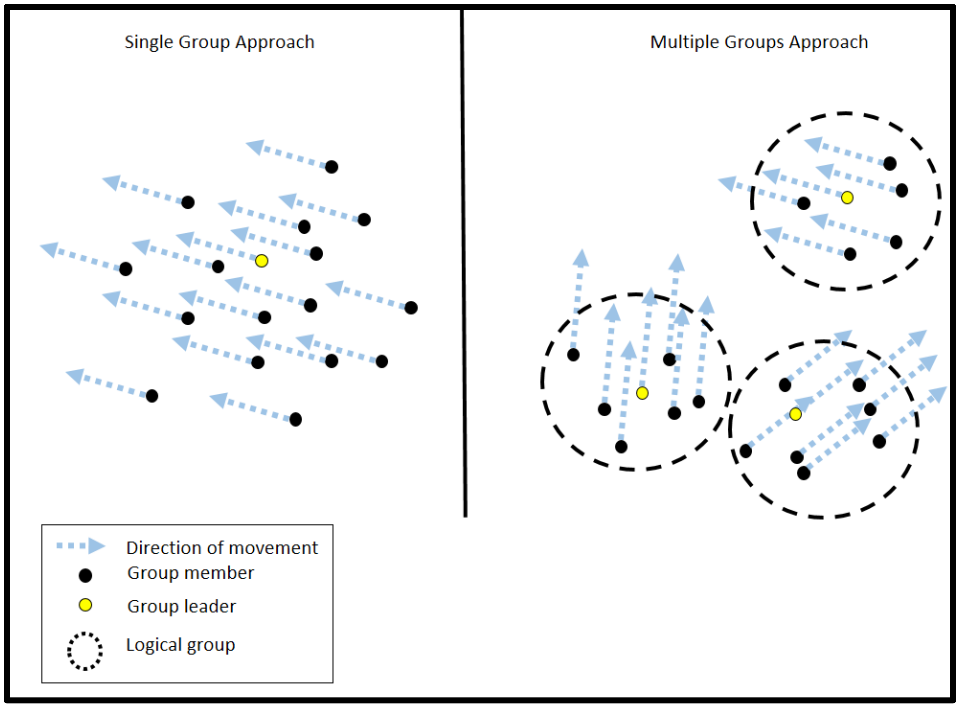


Figure 4. 3: group mobility model

The second mobility form is the group mobility, figure 4.3 above illustrates the mobility form. Each group of nodes has a logical group leader which leads the movement behavior of all members in its group, each node within the group derives its speed and direction from the group leader, where group leader set its speed and direction randomly.

In group mobility pattern, two approaches could be applied, the single group approach, where all the nodes in the network derives its motion pattern from one group leader and follows its way of mobility (direction angle deviation ration and speed ratio). The other approach is the multiple groups approach where multiple groups is formed leaded by multiple group leaders, each node joins one logical group and follows its leader and derives its motion velocity and direction. This pattern is useful in application like battle fields where units moves in groups followed by a single leader.

The other two forms are geographically restricted, that is, nodes moves within restricted maps that represents streets, the first form is the freeway model where nodes are bounded to its dedicated lane of the street, and the speed is dependent on its previous speed, and when 2 nodes are on the same lane the following one can’t exceed the speed of front one figure 4.4 (B) shows the freeway movement pattern.

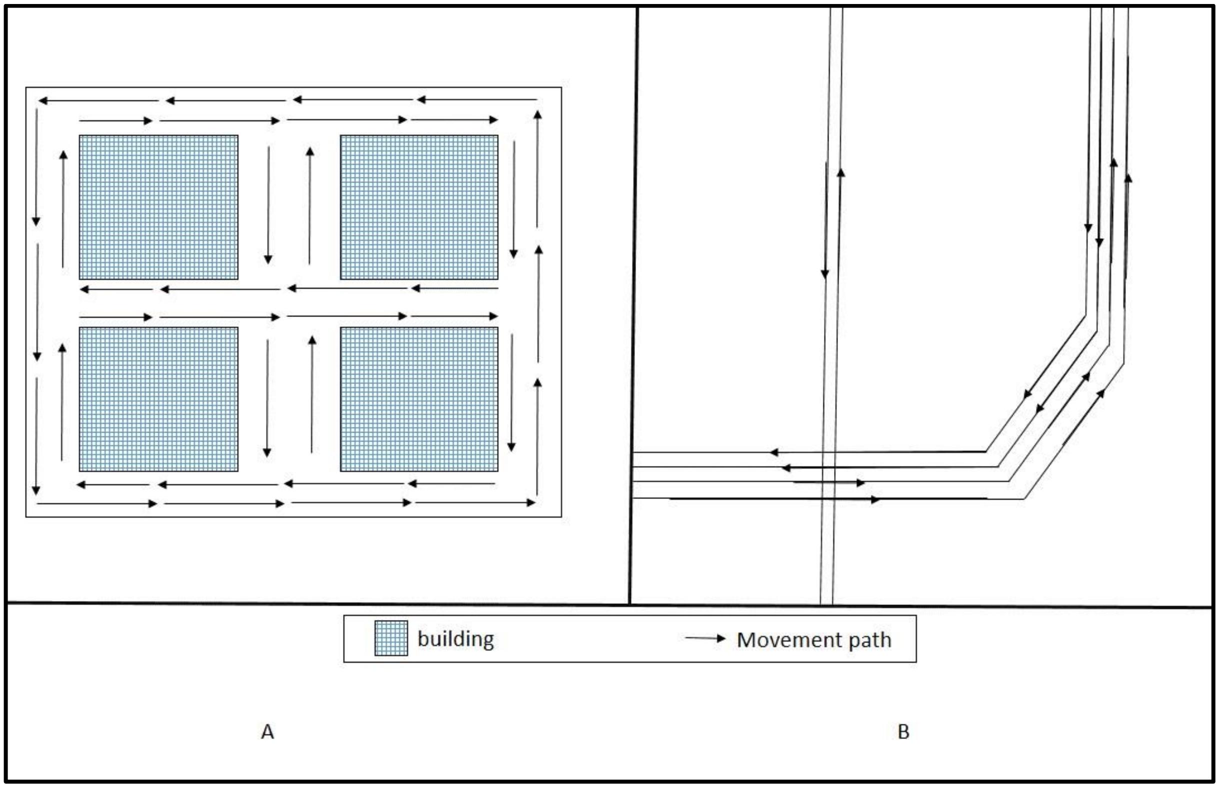


Figure 4. 4: (A) Manhattan mobility model, (B) freeway mobility model

Figure 4.4 (A) shows the Manhattan movement model, it is similar to freeway movement path that nodes moves in lanes in the street, the difference is that each node can make turns between buildings and returning to a lane that it used before, and also there is a probability that a node may continue on the same lane or turn left or right.

In our simulations we used the Random Way Point model, we want to simulate real world situations where mobile devices moves randomly in unexpected fashion, and hence we used the random waypoint positioning and motion, moreover, we used a pause time greater than 0.

4.2.4 Power

When simulating mobile ad-hoc networks, the power parameter is very important as any mobile device is powered by limited power source such as batteries, and all operations rely on that limited battery power. The power consumed when any node wants to for example send data, or receive data, even when devices are idle, power also consumed in wireless environments for listening to the media channel.

We explained the power consumption equations in (section 4.2.1). In IEEE-802.11-based routing specially in multi-hop networks, the routing protocol must be aware of power consumption and tries to save the power of nodes as possible. Another technique in saving power is transmission power control where transmission occurs based on need per node. The power aware routing could be applied by weighting routes based on remaining energy of intermediate nodes, either by calculating the total remaining energy or considering the power usage of each node.

4.3 Performance evaluation:

We used NS-2.35 to evaluate four of the routing protocols, two reactive protocols (AODV and DSR) and two proactive protocols (DSDV and OLSR). We aim to study the reactive protocols compared with proactive protocols, and also comparing the different reactive protocols with each other and also different proactive protocols with each other, and which protocol is better under specific conditions.

In our simulations we used the following tools and configurations:

1- Network Simulator (NS) version 2.35.

2- Ubuntu operating system version 14.04 over VMWare workstation version 9.0.2
3- Intel Core i7-2670QM @2.2GH processor, and 8GB memory
4- NS2 visual trace analyzer version 0.2.72

Some of the results are collected using NS2 visual trace analyzer that gives some of the desired information, and other information are collected using AWK files that reads the trace files and calculates some results, and some of the information are collected by manually studying the trace files.

4.3.1 Performance metrics:

In MANET routing, several performance metrics are interesting to be studied and compared among all tested routing protocols [46], these metrics gives a good indication about the performance and we can use these metrics as comparison parameters. The performance metrics measures the quantity and quality of service provided by the routing protocol. We explain each of these metrics briefly:

4.3.1.1 Throughput:

It is very important to measure the quantity of service being provided by the routing protocol, this could be calculated using throughput. Throughput is the amount of data that is delivered successfully from any given source to any given destination over specific period of time. In our simulations we calculated the average throughput of the tested routing protocols, we calculated the total amount of data received by the destination node at every second of the simulation time, and then we calculated the average throughput for all throughputs, the result is the average end-to-end throughput for the entire network for all destinations.

4.3.1.2 end-to-end delay

The end-to-end delay or one way delay is the amount of time required for a packet to travel from its generating source to any specific destination, this measurement gives us an indication about the quality of service that the routing protocol provides. This metric is different from the Round Trip Time (RTT) which means the time to go and come back from source to destination.

In wireless communications, there are several factors that affect the end to end delay, but generally we can calculate the end to end delay by using equation 4 below:

$$D_{end-end} = N[d_{trans} + d_{prop} + d_{proc} + d_{queue}] \quad (4)$$

Where:

$D_{end-end}$: end-to-end delay

N: number of links (number of nodes – 1)

d_{trans}: transmission delay

d_{prop}: propagation delay

d_{proc}: processing delay

d_{queue}: queuing delay

Each node will have its own delay, but in our case, all nodes will have the same transmission, processing, propagation and queuing delay, the difference will be in number of links or number of routers used. The routing protocol behavior affects the end to end delay when building up its routes and how packets are treated within each node, and also by the number of nodes it select to send data packets. We calculated the end-to-end delay by averaging all delivered packets delays.

4.3.1.3 Delivery ratio

Packet Delivery Ratio (or packet delivery fraction (PDF)) is the percentage of the total packets received by all receiving clients to the total number of generated and transferred packets sent by all source nodes. We can calculate the packet delivery fraction using equation 5 below:

$$PDF = \frac{\sum P_{recd}}{\sum P_{sent}} \qquad (5)$$

Where:

PDF: packet delivery fraction.

P_{recd}: total packets received by all destinations.

P_{sent}: total packets sent by all sources.

Sending nodes are set to send data packets at predefined rate called the packets rate, measured in packets per second, and each source will generate data packets and send them during the simulation time. Each node receives any packet will forward it to the next hop based on the routing entries stored in its own routing table or routing caches. The delivery ratio is the result of packet drop, packets are dropped and lost due to several reasons [47]. Most of reasons are due to buffer limitation and time-outs that forces the node to drop packets, for example, if a packet arrives to a node with full buffer, the node cant store that packet and will drop it, also, when a packet exceeds the time limit to be stored in the buffer, it will be dropped, because some routing protocols determines a time out limit for storing a packet in the buffer. Routing protocol stores the data packets in a buffer because it first needs to look for a valid path entry in its own routing table, and when no valid path is found, the routing protocol will wait for specific period of time until it found new one. Moreover, packets are lost due to congestion on the MAC layer, for example when the wireless channel is busy at the time of back off. Another reason is during the channel queue is full, any new arriving packet will be dropped.

4.3.1.4 Number of routes

Each routing protocol will search for paths to send packets from source to destination, these routes are selected based on the routing algorithm each routing protocol use, the number of paths that any specific protocol uses during the simulation time is called the number of routes metric. During the simulation time, the protocol may decide to use multiple routes during transmission process. We choose the number of routes as a performance metric because we want to measure the protocol utilization of nodes in the network, does the protocol uses too many nodes to deliver packets, or it keeps using the same set of nodes. Moreover, number of routes gives us a good indication of routing protocol adaptability to topological changes, i.e. the mobility factor may cause the network routes to expire very fast, and hence the routing protocol needs to discover and use alternate routes to cube these changes in the topology. And also, using less number of routes, mean the routing protocol is exhausting specific routes rather than distributing the load to all nodes in the network. So it is very interesting to measure the number of routes metric.

4.3.1.5 Network lifetime

The network life time metric is the period at which all sources in the network are still able to transfer data to destinations. This period of time is affected by the nodes life time, i.e. when the routing protocol decides to send data it will use some of the intermediate nodes to forward data packets, by the time some of these intermediate nodes will run out of energy and will not be able to forward packets, at this time, the routing protocol will search for an alternate route to transfer data, this process of alternating routes will continue until all intermediate nodes forming these routes are out of energy and no other alternate routes exist, then the network will stop and fails to deliver data by any mean. The entire time that the network is able to send and receive data packets is called the network lifetime.

Another related important metric, is individual nodes lifetime, which is the time form the beginning of simulation until the node consumes all of its energy. This metric gives us an indication of protocol utilization of nodes and how the protocol distributes the work load among all nodes within the network. For example, if all nodes are set to have the same initial energy level, the routing protocol may rely only on specific set of nodes and consume its energy, leaving other nodes in the network partially unused.

Chapter 5: Experimental study of AODV, DSR, DSDV, and OLSR routing Protocols

5.1 size of the network (network density)

The size of the network represents the number of active nodes that participate in the network events and activities. The problem with the size of the network that it is directly affected by the scenario used to make a connection between a sender and receiver. The only thing we can deduce from the simulations we did on the size of the network is that it does not give any information in terms of the performance of the protocols.

The smaller the size of the network means less neighbors around each node or even no neighbors, this affects the connectivity of the entire network as some nodes may be out of reach and will remain out of reach when the nodes mobility is 0. The results of the simulations shows that the connectivity of the network affected by the mobility of nodes, the chance for an “out-of-reach node” is higher to be reached when it is or other nodes are moving.

In the following figure 5.1 represents the effect of large networks compared to small networks. The 2 scenarios uses an area of 1000X1000 m, the nodes in (a) has lower degree of connectivity with their neighbors for example node 5 (red) in the upper right corner has only one neighbor. Low dense networks make the network more prone for out of reach situations like node 9 (blue) in the upper center. While in (b), the nodes have higher degree of connectivity; that is, each node has larger number of neighbors, like node 5 (red) in the upper right corner, the node has 8 neighbors. For node 9 (blue) still out of reach for the entire network, things will get worst if the nodes are not moving (mobility is 0) as node 9 will stay out of r each all the time.

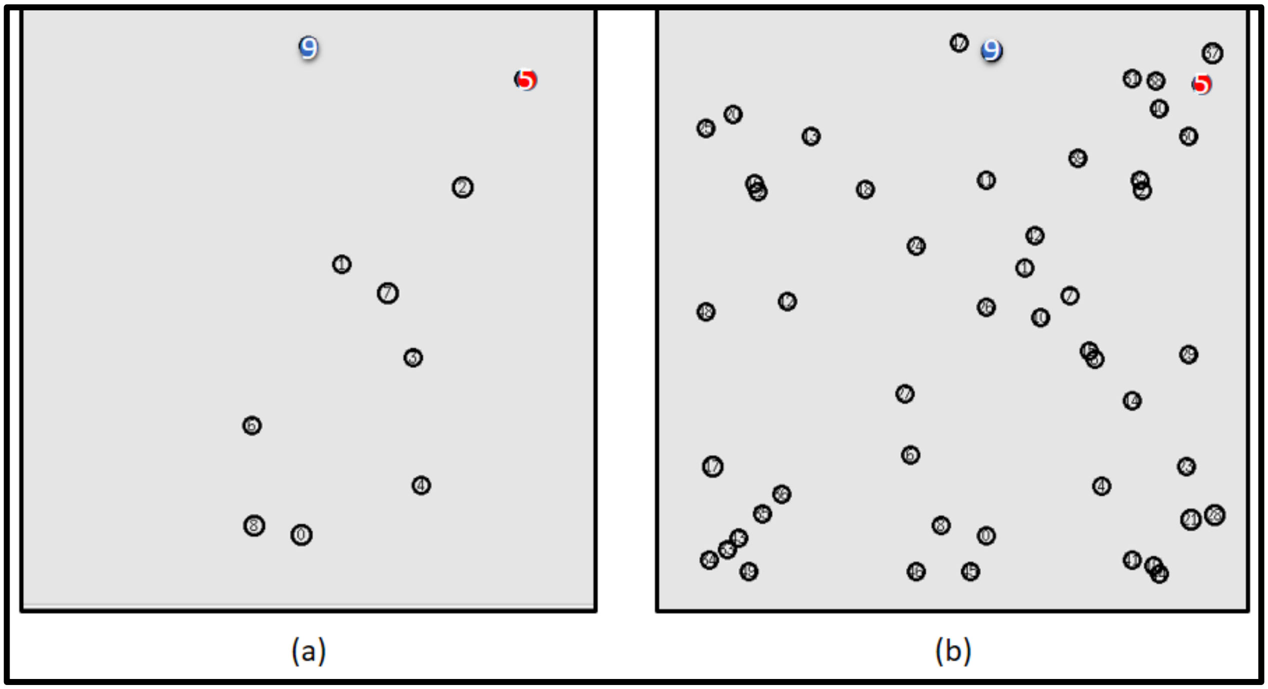


Figure 5. 1: Network density example, (a) low dense network, (b) high dense network

5.2 speed of nodes (mobility)

The mobility of nodes represent the speed of nodes that moves within the topology defined in the simulation. In real world scenarios, the wireless devices are most of time mobile and keep moving in unpredicted way. To simulate the unpredicted form of movement, we used a random way point movement where nodes move in random way and in different speeds with maximum defined speed measured in meters per second. For example if the maximum speed is set to 1 meter per second then the nodes will move in random directions with a random speed in the interval [0.0, 1.0] m/s. this means that each node may change its speed and direction at any time during the simulation, this behavior is required to simulate the real world scenarios as mobile devices is meant to be mobile all the time.

Generated scenarios are all the same except the speed of nodes. We varied the speed from 1m/s which represents the human slow walk to about 20m/s which is the average speed of vehicles. The mobility was randomized among all nodes in the network, the resulted randomized mobile nodes scenario has unreachable nodes during the simulation time, and this is also required as a result of mobility and also simulates the real world scenarios.

Another important parameter in mobility is the "pause time", which is the time between successive movement events for any specific node, [NS2 manual]. For example, in our experiment we set the speed of nodes in the range [0.0, 5.0] m/s, after any node moves to a new position in a speed within that specified interval it stops in the new position for "pause time" seconds before it moves to another new position. In our experiment we set pause time to 1 second.

5.2.1 Experiment setup

To study the behavior of routing protocols in dynamic environment, we varied the speed of nodes and generated different scenarios for every routing protocol. We produced 20 scenario files, 5 scenarios for each routing protocol, every scenario differs in maximum speed where nodes moves in a speed within the interval [0.0 – 5.0] m/s. The number of nodes in the network is constant for all scenarios (50 nodes).

The mobility and initial positions of nodes are generated randomly by using "setdest" generator tool that is included in NS2 simulator package. The tool sets initial positions and movements of nodes within a predefined topology. For every speed we created different random initial positions and movement patterns and applied the same generated movement for all 4 routing protocols (AODV, DSR, DSDV, and OLSR), the same movement scenario for speed (5 m/s for example) is applied for AODV and the same scenario is applied for DSR, DSDV, and OLSR. In our simulation we used constant number of nodes which is 50 nodes and the grid size area is (1000 X 1000) m^2. The choice of such variation is due to unreachable destinations during the simulation time. I.e. during the simulation time a node may become isolated and out of reach for a specific period of time, the number of isolated nodes during the simulation time is represented as unreachable destinations. For our test purposes we need a scenario where a high dense network with minimum number of unreachable destinations as shown in table 5.1 below. We notice that using 50 nodes over an area of 1000 X 1000 m^2 produces the minimum number of destinations unreachable for all speeds. Speeds higher than 20 m/s shows almost the same value. Based on these tests we set the simulation speeds from 1 m/s up to 20 m/s and the number of nodes 50 and grid size area is 1000000 m^2 (1000 X 1000) where each node occupies an area of 20000 m^2. We excluded the 5-node selection because of the low density factor that each node occupies (200000 m2/node) and the destinations unreachable remains unreachable for longer time.

Table 5. 1: destinations unreachables for different number of nodes vs speed

speed	*5-nodes*	*10-nodes*	*20-nodes*	*30-nodes*	*40-nodes*	*50-nodes*
	density					
	200000 m^2/node	100000 m^2/node	50000 m^2/node	33333 m^2/node	25000 m^2/node	20000 m^2/node
0 m/s	7	23	67	131	0	0
2 m/s	10	29	100	189	0	0
5 m/s	10	39	158	238	0	0
10 m/s	11	59	197	352	155	98
20 m/s	15	118	214	331	154	49
35 m/s	25	142	462	870	177	49
50 m/s	48	191	681	1088	266	52

Before we set up the simulation parameters we tested up different varations between grid size and number of nodes and we found that the density factor (size / number of nodes) play the major role in affecting the scenario. For example, using 18 nodes over a grid area of 600 * 600 m will result the in the same unreachable destinations as using 50 nodes over a grid area of 1000 X 1000, because each node occupies a 20000 m^2 area in the 2 scenarios.

Table 5. 2: Mobility simulation parameters

Simulator	NS-2.35
Channel	Wireless-Channel
Propagation	Two-Ray-Ground
Interface	Phy/WirelessPhy
Queue	DropTail/PriQueue
Queue length	50 packets
Antenna	Omni-Antenna
Protocols	AODV, DSR, DSDV, OLSR
Simulation time	500s
Topology area	1000m X 1000m
Number of nodes	50
Transmission range	250m
Movement type	Random waypoint
Mac layer	IEEE 802.11
Pause time	1s
Max speed	1,5,10,15,20 m/s
Packet rate	5 packets/s
Data payload	512 Byte/packet
Traffic type	CBR

Also, we created 10 CBR flows that connects 10 pairs of nodes, i.e. 10 source nodes transmit data packets to 10 destination nodes. The data packets size and send rate are also defined, the packets rate and size represents the data payload in the network, in our experiment the size of each data packet is 512 bytes and the send rate is 5 packets per second. The same CBR flows is applied for all mobility scenarios for all simulated routing protocols. The connection flows are randomly generated by using CBR generator tool included in NS2 simulator package, by setting up the number of flows and the size of each packet, the resulted connection flows connects each pair of source and destination at random time during the simulation time. The complete parameters we used in this simulation is mentioned in the following table:

5.2.2 Throughput

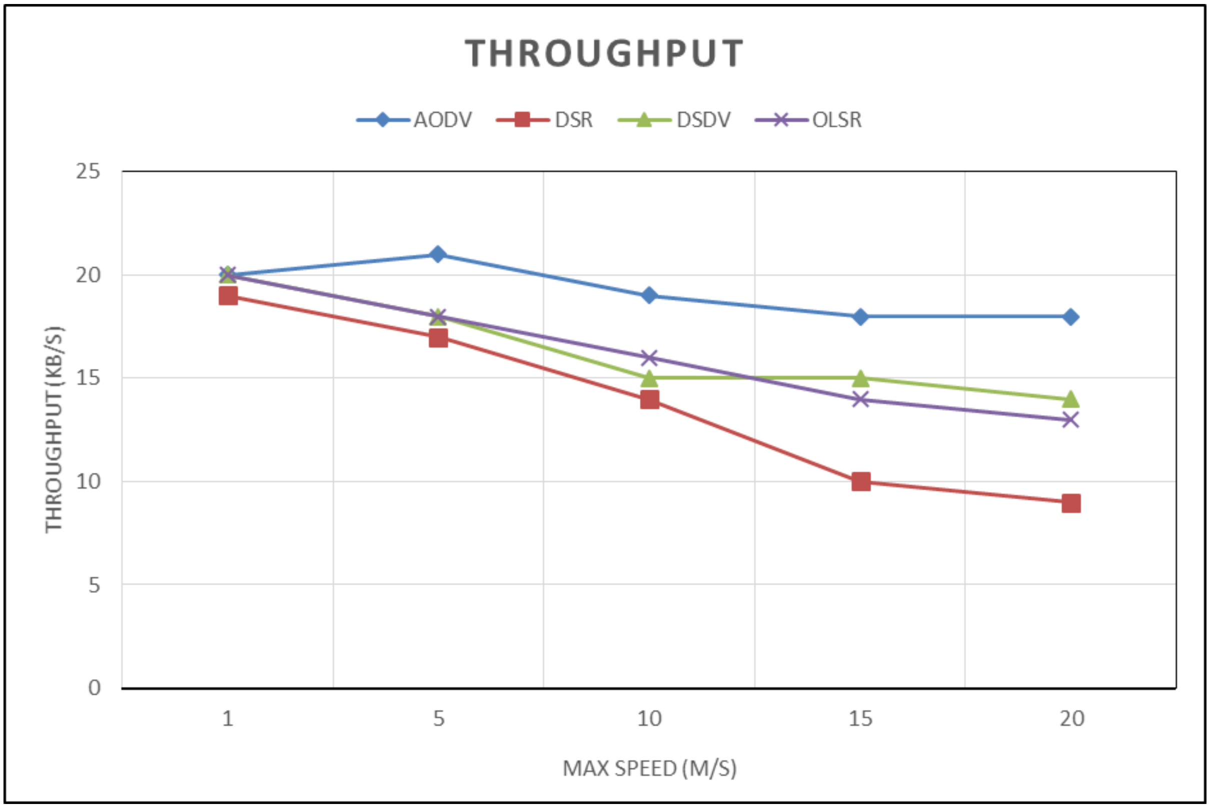


Figure 5. 2: throughput vs. speed for all routing protocols

Throughput is the amount of data that is successfully transferred from a source to the desired destination in any unit of time, and measured in bits per second or byte per second, etc... Figure 5.2 above shows the actual throughput of each routing protocol under the simulation parameters we set. We noticed that AODV protocol has the highest throughput among all other tested routing protocols for all speeds, except for 1 m/s mobility speed where all routing protocols shows almost the same throughput value. All routing protocols shows lower throughput as the speed increases, nearly all routing protocols performance decreases when speed is over 5 m/s. both DSDV and OLSR protocols shows nearly the same results, OLSR and DSDV are table-driven protocols and link breakages detection and maintenance mechanism takes more time than reactive protocols like AODV, and as a result the throughput of both protocols is less than AODV protocol. DSR protocol shows the lowest results although DSR is a reactive on-demand routing protocol like AODV. DSR aims to minimize the overhead but it is not efficient on large networks or on high mobility environments, the route maintenance mechanism does not repair local link breakages, and also there is inconsistence in the route reconstruction process due to cache information about routes. Moreover, DSR has higher delay when building up the connection than table-driven routing.

5.2.3 End-to-End Delay

The end to end delay is the time that it takes a packet to be delivered to its destination successfully, this time depends on nodes themselves and the links between nodes in addition to other several factors. Figure 5.3 below shows the average End-to-End delay for all simulated routing protocols. All AODV, DSDV and OLSR shows almost the same results in the delay, the protocol that has the highest delay is DSR for all mobility simulations. As we noticed, things become worse when increasing the speed of movement, where the delay increases dramatically for DSR protocol. While the rate of increase down less for the rest of the protocols. OLSR and DSDV shows better results even they are pro-active protocols, this is because the delay is calculated for a single packet when it is delivered successfully, but in case of OLSR and DSDV a lot of packets dropped before being delivered to destination, the packets that is delivered has lower delay as link breakages are discovered before packet is sent, while in AODV link breakages are maintained during transmission of packets and hence more time is needed to reconstruct the path and resume transmission.

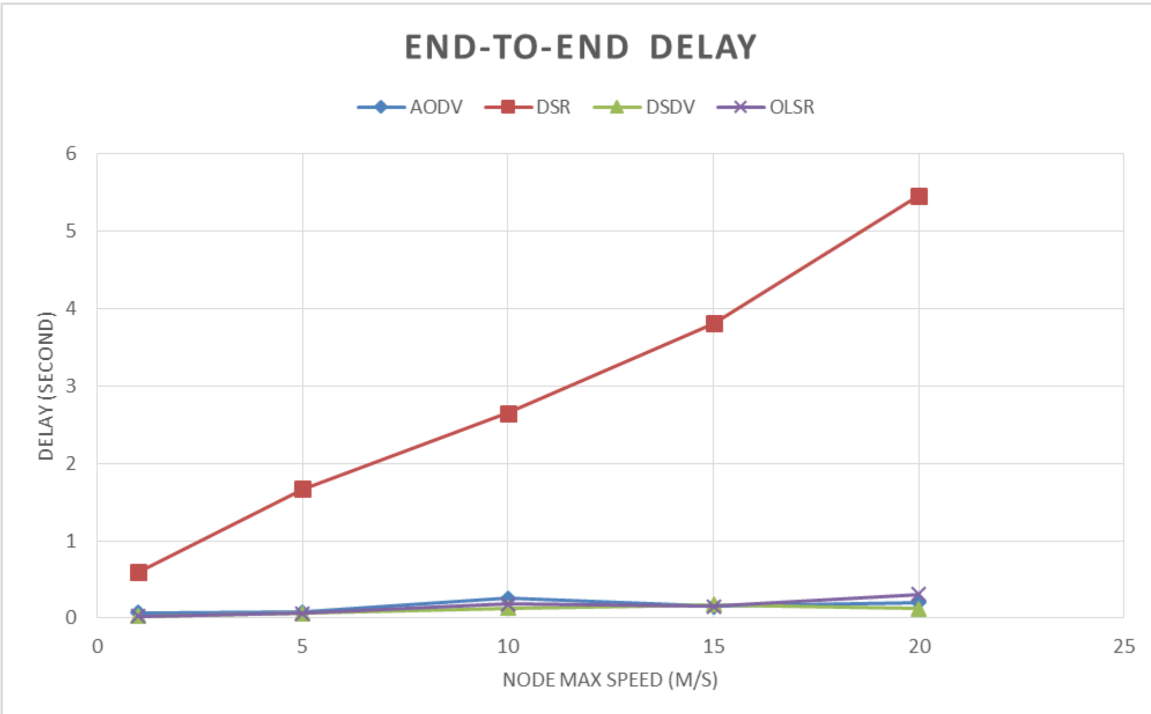


Figure 5. 3: End-to-End delay vs. speed for all routing protocols

DSR has the highest delay and as we notice the average delay is much higher (up to 3.8 seconds) compared to 0.25 seconds the highest average delay for the other protocols, the reason behind this delay is that DSR is source routing protocol where the path is calculated during any transmission process by listening to any received packet, and also the complete path is propagated along the route to destination which means higher packets size that needs more time to propagate to destination and hence the average increases. Another important reason is the buffering time, the buffer keeps the packets for longer time in DSR protocol until a valid route is found, and because of high mobility, maintaining new route takes longer time and the packet saved in the buffer until it is retransmitted again. DSR keeps the packet for 30 seconds while AODV keeps the packets in buffer for only 8 seconds, because of mobility link breakages will be higher and hence the need to hold packets in buffer increases.

5.2.4 Packet Delivery Fraction (PDF)

Packet delivery fraction represents the ratio between transmitted packets and successfully received packets, in our simulation we set the sender node to transmit 5 packets per second, not all generated packets are delivered to the destination, some of those packets are dropped for different reasons. Figure 5.4 below shows packet delivery fraction for all tested routing protocols.

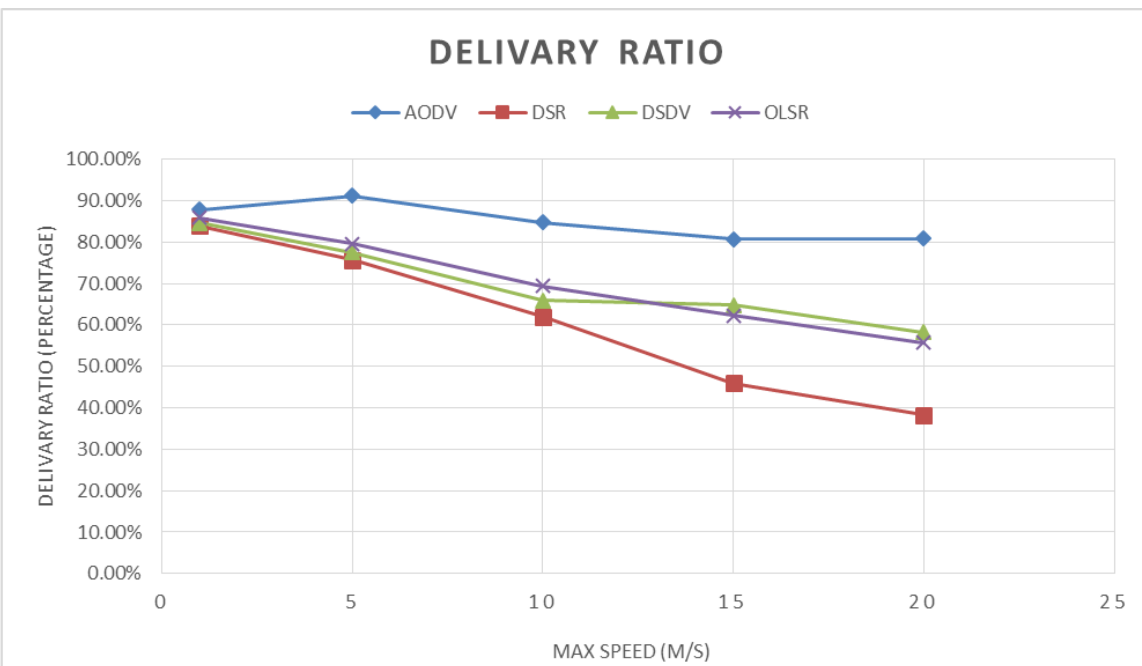


Figure 5. 4: Packet Delivery Fraction vs. speed of nodes for all routing protocols

We notice that increase in mobility also decreases the packet delivery ratio, the reason for this packet loss is that protocols try to send packets using invalid or broken links before it is aware of the changes of the network because of mobility. AODV routing protocol shows better results, up to 87.83% of generated packets are delivered to their destinations. AODV can maintain routes during transmission of packets on-demand, and hence lower number of packets are dropped due to timeout in the send buffer. DSDV and OLSR are proactive protocols, and need more time to be informed and reconstruct routes to destination. Most of packets are dropped because the routing protocol try to send packets using a broken link before maintaining another route and rebuilding routing table.

DSR protocol again shows lower packet delivery ratio especially when speed exceeds 10 m/s. DSR routing mechanism make use of eavesdropping of packets in the network, complete route is included in the transmitted packets and information of the route is embedded in the packet, the neighboring nodes stores information about the route in its cache and tries to use these information to forward packets, but because of high mobility, those information become invalid quickly, when any node wants to forward a packet, it will use the cached information which it is not yet aware of its expiration, and hence that packet will be dropped.

Increase in speed means increase in like failures and hence more and more packets will be potentially dropped and not delivered to destinations. Another factors that affect the delivery fraction, one is collisions, propagation, and timeout in sending buffers.

5.2.5 Number of Routes

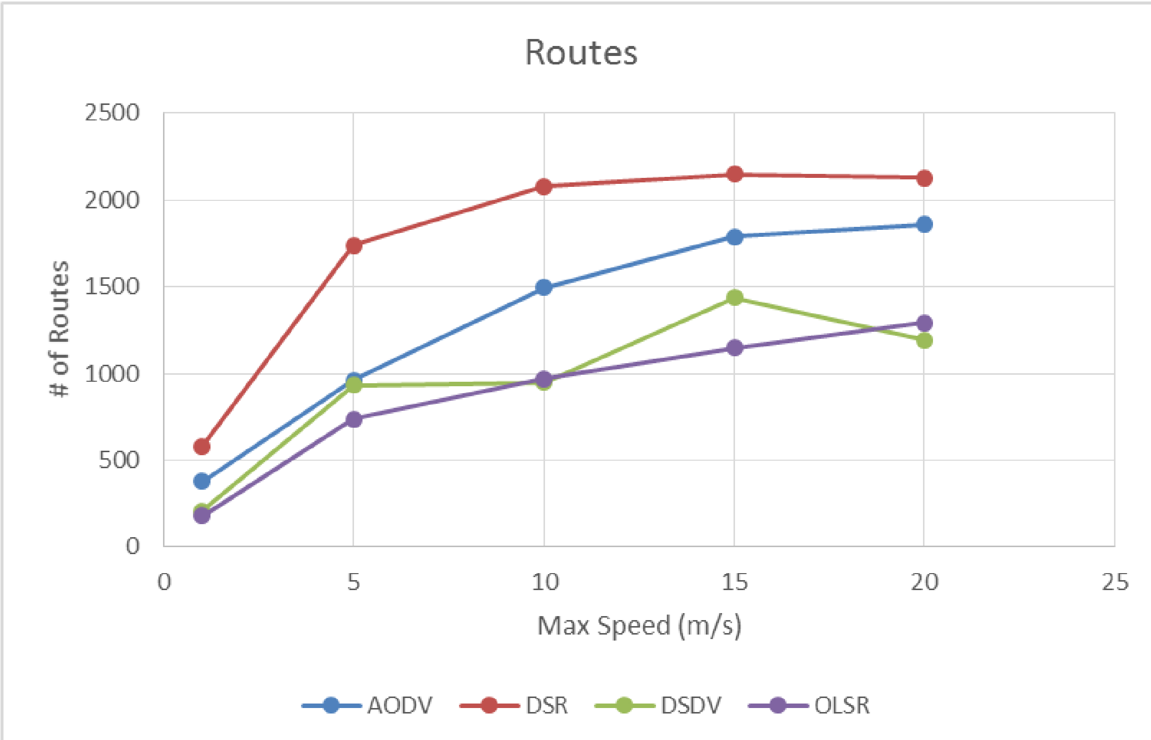


Figure 5. 5: number of routes vs. speed for all routing protocols

Figure 5.5 above shows the number of routes used by each routing protocol during the simulation time to transmit data from sources to destinations. We notice that by increasing the speed of movement, the number of routes used by each protocol also increases. Proactive protocols DSDV and OLSR uses lower number of routes than reactive protocols. Reactive protocols AODV and DSR are more aware of routes failures and hence can use more routes as quick as the route fails, while DSDV and OLSR takes longer time to discover failures and keeps using the same route. When any link break occurs, AODV quickly resend a route request message (RREQ) to find a new route, while in DSDV for example, depends on periodic update of routing table, the sender node will keep using the same route until a failure message received indicating a link break, then the sender will trigger a failure and look for different route.

DSR protocol uses the largest number of routes, up to 2173 different routes for all 10 flows. The reason is that DSR uses that much routes to deliver packets is the extra information it get from overhearing, DSR gets more information about link changes in the network, and because of high mobility of the nodes, more information is exchanged and updated in the nodes, and DSR switches for different routes quickly.

The number of routes used is an important factor in evaluating MANET routing. Dynamic topologies with high speed requires the routing protocol to be quickly adaptive to those changes as well. Proactive protocols like DSDV and OLSR are less adaptive to topological changes as it requires more time to update its routing tables because of periodic broadcasts and as a result a lot of packets are dropped because of high rate of link breakages. Reactive protocols like AODV and DSR are highly adaptive to topological changes.

5.2.6 Routing Overhead and Normalized Routing Load

Overhead represents the total number of control messages that the protocol uses to achieve its mission, those control messages are needed to find routes to desired destinations and also required to make maintenance to broken routes by informing other nodes for the failures and finding alternate routes. Figure 5.6 below shows routing overhead for all 4 routing protocols. We only calculated the routing overhead not the MAC layer overhead or the physical layer overhead because we only want to evaluate the protocol mechanism of routing and not the implementation side of each network layer of IEEE 802.11 specifications.

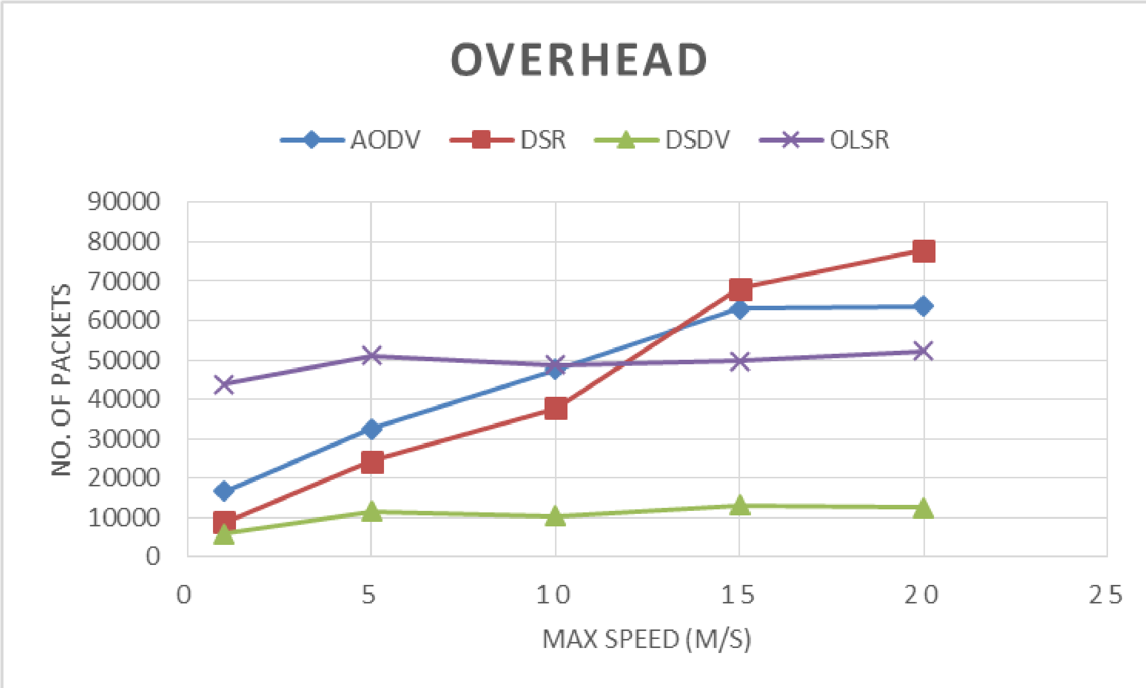


Figure 5. 6: routing overhead vs. speed for all routing protocols

DSDV routing protocol uses the lowest number of routing packets among all routing protocols, and also the number of routing packets almost constant even on high speed movement. DSDV and all other proactive protocols like OLSR depends on periodic update of the routing tables, and as a result the total number of routing packets are almost constant for the same period of simulation time, the total number of packets for DSDV varies from 6K up to 13K routing packet on extreme speeds, while OLSR varies from 43K up to 52K on high speeds. on the other hand, reactive protocols shows higher values when the speed increases and the variance in the number of routing packets is high, total number of routing packets for AODV varies from 16.7K up to 63.1K on high speeds, and also for DSR the total number of routing packets increases significantly when speed increases, number of routing packets on low speed is 6K and rises up to 68K on extreme mobility conditions.

Mobility causes high rate of topological change and as a result high number of link breakages occurs frequently, the routing protocols keeps trying to maintain those changes. DSR and AODV are reactive protocols, when any route fails, the protocols directly triggers route error message informing about that failure and resend a route request message, these frequent error and route request messages explains the big difference from DSDV protocol, DSDV only updates the routing tables upon periodically broadcasting control messages informing links states. OLSR shows higher values of routing overhead from other routing protocols especially on relatively low speeds (less than 10m/s), but the value almost constant for all movement speeds, OLSR depends on periodic update of the links state, but it differs from DSDV is that it depends on multipoint relay (MPR) nodes, those nodes are responsible for communicating with other neighboring nodes, this will increase the number of control messages especially over dynamic topologies.

It is also interesting to measure the number of routing messages needed to deliver one data packet, this is called Normalized Routing Load, we can calculate normalized routing load by dividing the total number of routing packets over the total number of delivered packets

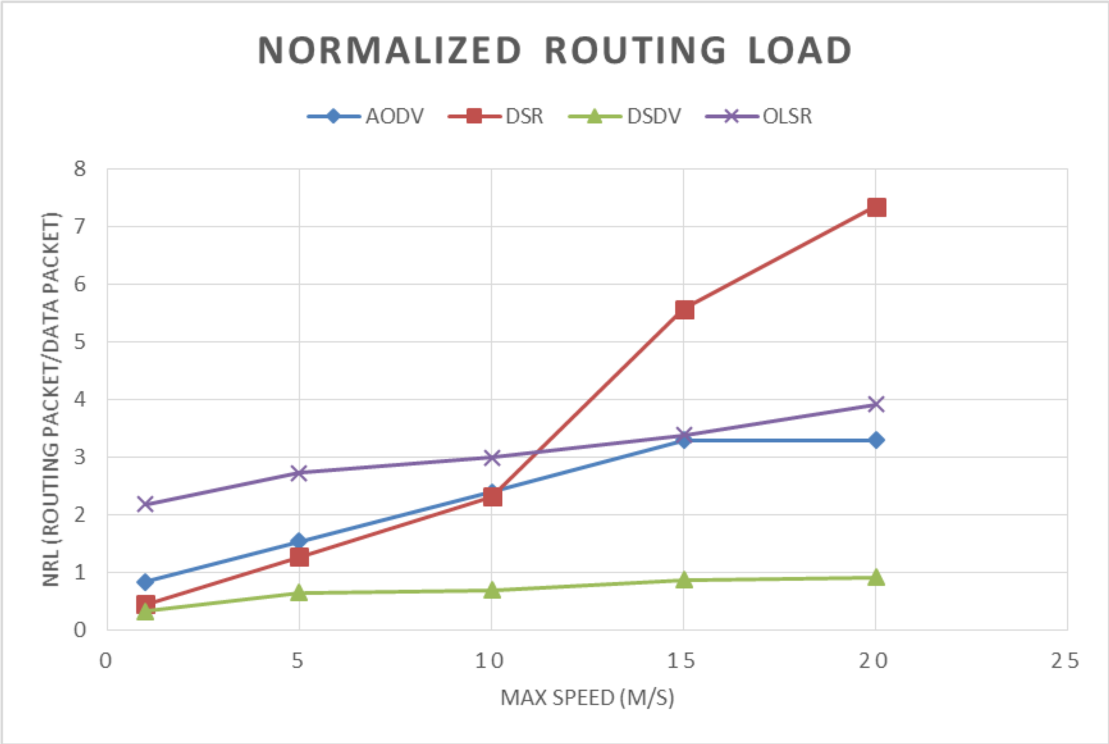


Figure 5. 7: NRL for all routing protocols under all mobility speeds

Figure 5.7 shows the normalized routing load (NRL) for all tested routing protocols, we notice that proactive protocols (DSDV and OLSR) has minor constant increase in the routing load which means almost the same number of routing packets needed in all speeds, but the data delivered decreased and hence the total number of routing packets needed to deliver the same amount of data packets increased. For example, DSDV at speed 1m/s needs about 0.31 routing packets for a single data packet to be delivered, this value increases when speed reaches 20m/s where the protocol needs about 0.86 routing packet for each data packet, the increase ratio is 277%, the same goes for OLSR with a ratio of 160%. These results because DSDV and OLSR are not fully aware of the network topological changes and keeps using the same number of routing packets under any condition. The other 2 reactive protocols shows major jumps in the routing load, because these protocols are more aware to topological changes, and any change in the topology increases the number of routing packets needed to deliver the same amount of data packets. For example, AODV at speed 1m/s the total number of routing packets per data packet is 0.83 and on high speeds over 10m/sit reaches up to 3.28 routing packet for each data packet, the increase is about 390%. The worst protocol is the DSR protocol where it needs about 0.43 routing packet for 1m/s speed to deliver one data packet and up to 5.57 routing packets to deliver one data packet for speeds greater than 10m/s with a major increase of 1290% which is a huge value, this is due to DSR mechanism of routing, where the protocols fails in the high rate of topological changes and in the networks where hops are greater than 10 nodes, and the need for routing packets increases on large and high dynamic networks.

5.3 Power Consumption

The power consumption metric is an important factor in evaluating MANET routing protocols. MANET protocols are supposed to guarantee a high degree of connectivity between nodes under extreme conditions where the power source is limited. The lifetime of the nodes and the lifetime of the entire network is extremely important in MANET routing.

We will study the performance of routing protocols in terms of power consumption. The effect of routing protocol over individual nodes and over the entire network are studied in 2 scenarios for all the 4 routing protocols (AODV, DSR, DSDV, and OLSR). The first scenario aims to measure individual node power consumption. This metric is important, node should be alive as longer time as possible, this will enhance the connectivity of the entire network and make sure all destinations are reachable from any source.

5.3.1 Individual node

5.3.1.1 Simulation setup

The scenario used to measure individual node is shown in figure 5.8. We used a single CBR flow to connect the sender (node 0) to the receiver (node 1). We supposed that node 0 and node 1 have unlimited power, and the intermediate nodes are varied in power levels. In this scenario we want to evaluate the power consumption for the intermediate nodes that used by routing protocol to deliver packets from source to destination and how the protocol will behave when different paths and different energy levels exist in the network.

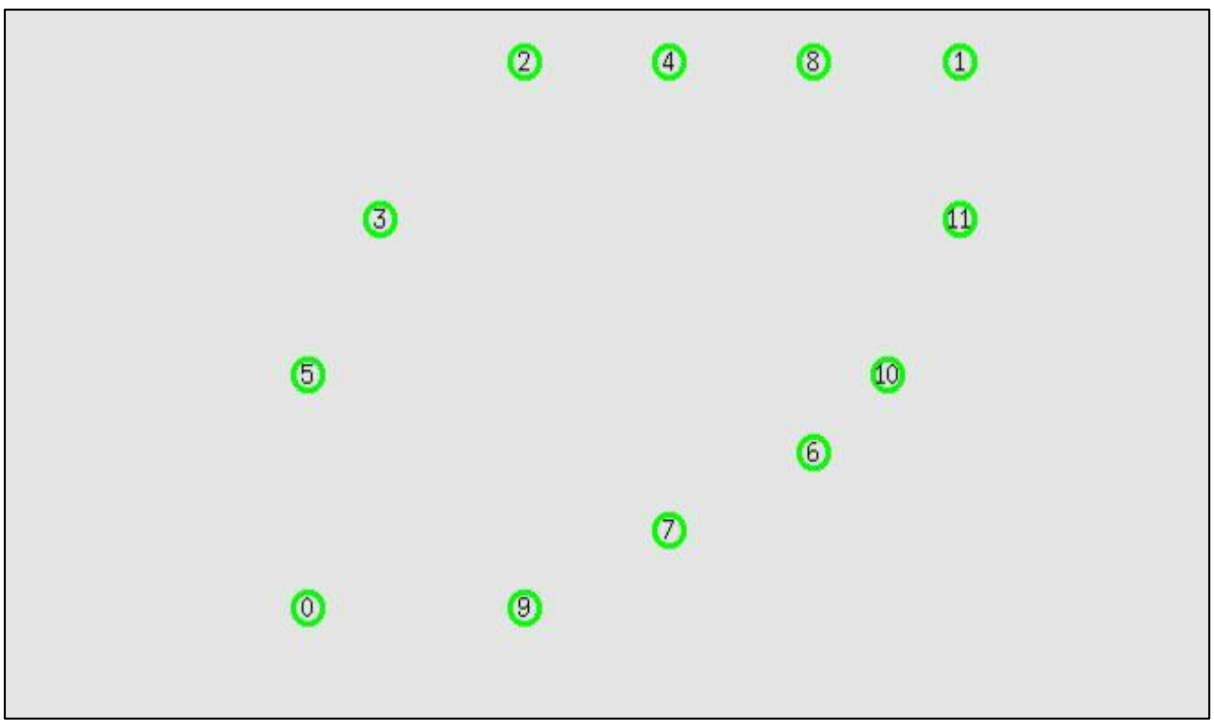


Figure 5. 8: simulation scenario for individual node lifetime

The power levels for nodes (5,3,2,4,8) are 7 joules each, and for nodes (9,7,6,10,11) are 15 joules each. The reason behind varying the power levels this way is to make sure that the first group of nodes will die earlier than the second group and to make sure both routes will be used. To further illustrate, there are only two available routes from source 0 to destination 1, we want to analyze the routing protocol behavior in such scenario in terms of power consumption. The complete parameters used in the simulation scenario are shown in table 5.3 below:

Table 5. 3: simulation parameters for node lifetime

Simulator	NS-2.35
Protocols	AODV. DSR. DSDV. OLSR
simulation time	60s
simulation area	500 X 400 m
number of nodes	12 nodes
transmission range	250m
mac layer	IEEE 802.11
data payload	1024 bytes/packet
traffic type	CBR
# of flows	1 flow
Rx Power	0.2 W
Tx Power	0.9 W
Idle Power	0.01 W
Sleep Power	0.001 W

The energy consumed by each node in MANET when it is active. The power is wasted in several modes, the transmission mode when node wants to send packet, receiving mode also consumes power when node receives a packet. The other two modes are the idle mode and sleep mode [39]. The energy of each mode is calculated by the formula [38]:

$$E = P \times T$$

Where E: is the energy consumed.

P: is the mode power

T: is the time required for transmitting k bits.

We assumed that all nodes uses IEEE 802.11 interface and the power values are user specified (for transmitting is 0.9 Watt and receive power is 0.2 Watt, idle power is 0.01 Watt and sleep power is 0.001 Watt). The transmission range of each node is 250 m and the topology area is 500X400 meters.

5.3.1.2 Simulation results and analysis

We first evaluate the protocols behavior in terms of remaining energy, the remaining energy of each node is shown in figure 5.9 and 5.10.

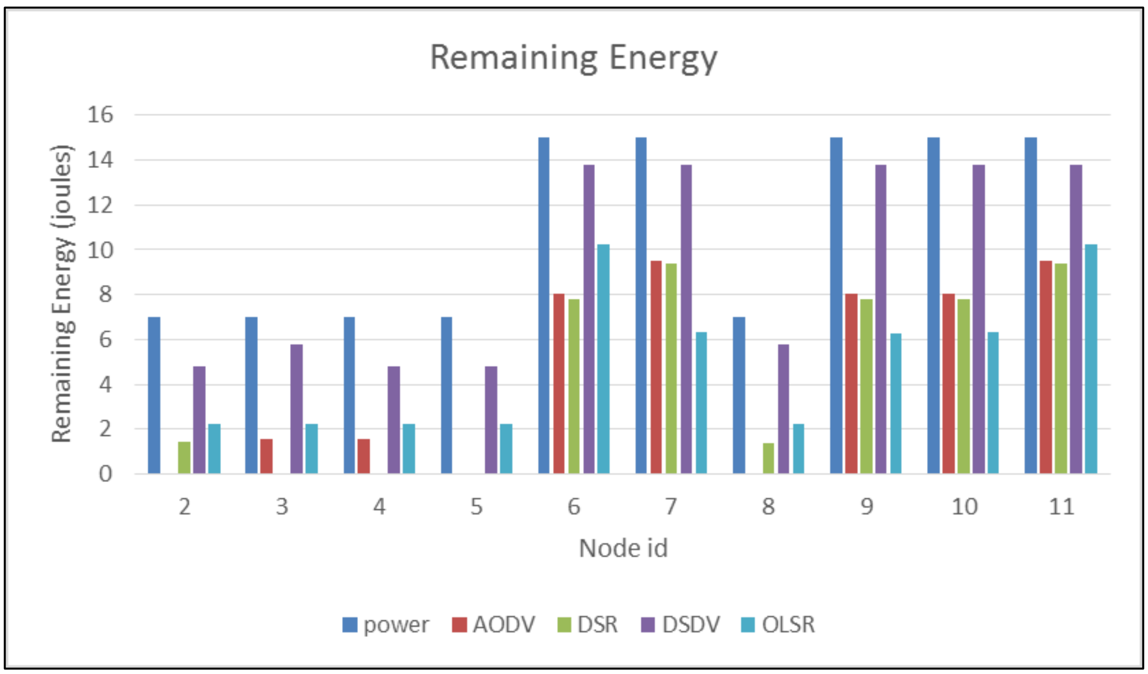


Figure 5. 9: Remaining energy for all nodes in the network

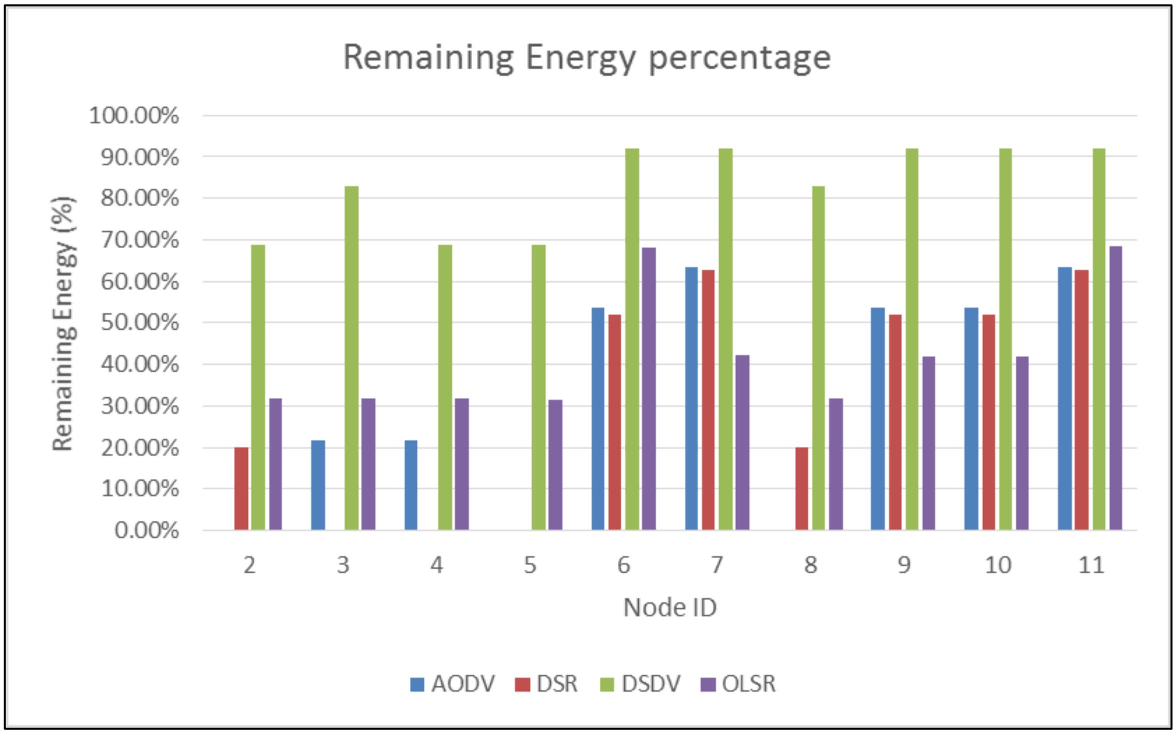


Figure 5. 10: remaining energy percentage of all nodes in the network

The remaining energy of each node varies depending on the original initial energy of each node and also whether it participated in the routing process or not. For the first set of nodes (2, 3, 4, 5, and 8) that the protocols used as a path to send data from source to destination has consumed most of the energy it has and some of nodes died, actually the routing protocols continued using this route until it became invalid as some intermediate nodes died. All the 4 routing protocols (AODV, DSR, DSDV, and OLSR) behave the same, it consumes 2 to 3 nodes of the first route until the route becomes invalid then it uses the other set of nodes until the end of the simulation.

AODV and DSR protocols started transferring CBR packets at time 0.1 second from the beginning of the simulation, the transmission process lasts for about 60 seconds, while OLSR protocol started transferring data at time 10.2 second from the beginning of the simulation, the connection last for about 50 seconds. And finally for DSDV protocol the routing began at time 49.5 and lasts only for about 10 seconds. The delay in transmission that DSDV and OLSR have is necessary as those protocols are proactive ones and needs more time to build up its routing tables before it can start transmitting data packets. The result for this behavior, the amount of energy consumed by nodes is less because the data transmission period is less as shown in fig 5.9 above.

The remaining energy percentage (fig 5.10) shows the percentage of remaining energy from the original initial energy of each node. Some nodes died with 0 percent of the original energy that it have, and some other have little remaining energy percentage. This applies to all the protocols used in the experiment except for DSDV because of the reasons we explained before. The nodes, which were used for less time during the process of sending data has kept a higher percentage of remaining energy.

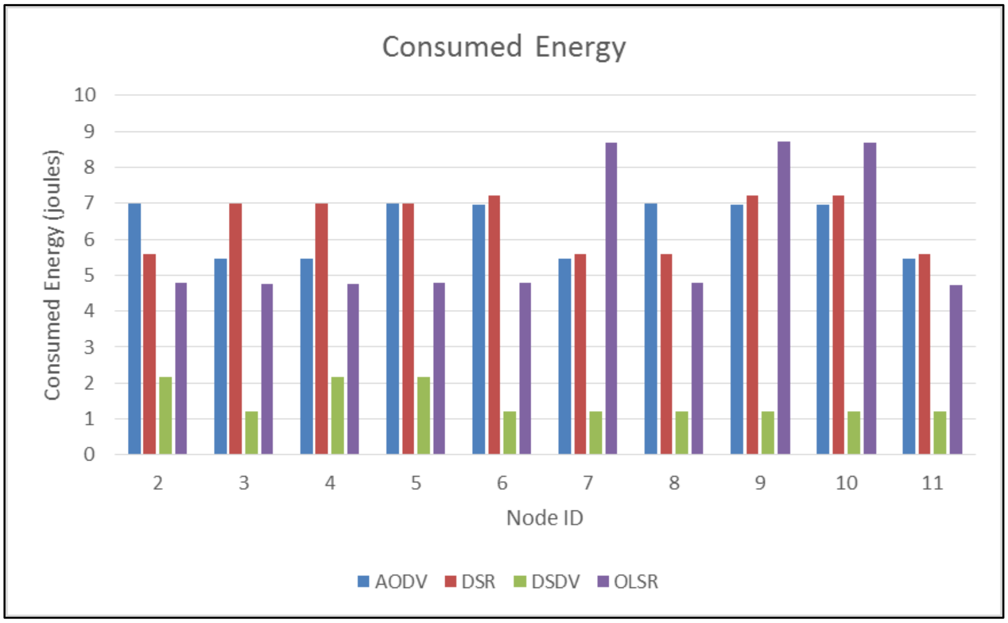


Figure 5. 11: Consumed energy for all nodes in the network for all routing protocols

Fig 5.11 represents the consumed energy for every node in the network. From the figure we noticed that some nodes consumed more energy than other nodes and also some nodes consumed the same amount of energy during the entire simulation time. For example, AODV protocol used the first route from source to destination (fig 5.8 above) using nodes (source-5-2-8-destination). The intermediate nodes consumed all of its power (7 joules). Node 3 and node 4 consumed most of its energy although they did not participate in the routing process, this is because of idle power consumption and overhearing consumption, where the nodes in the transmission range of participating nodes consumes most of its power in listing to their neighbors[40].

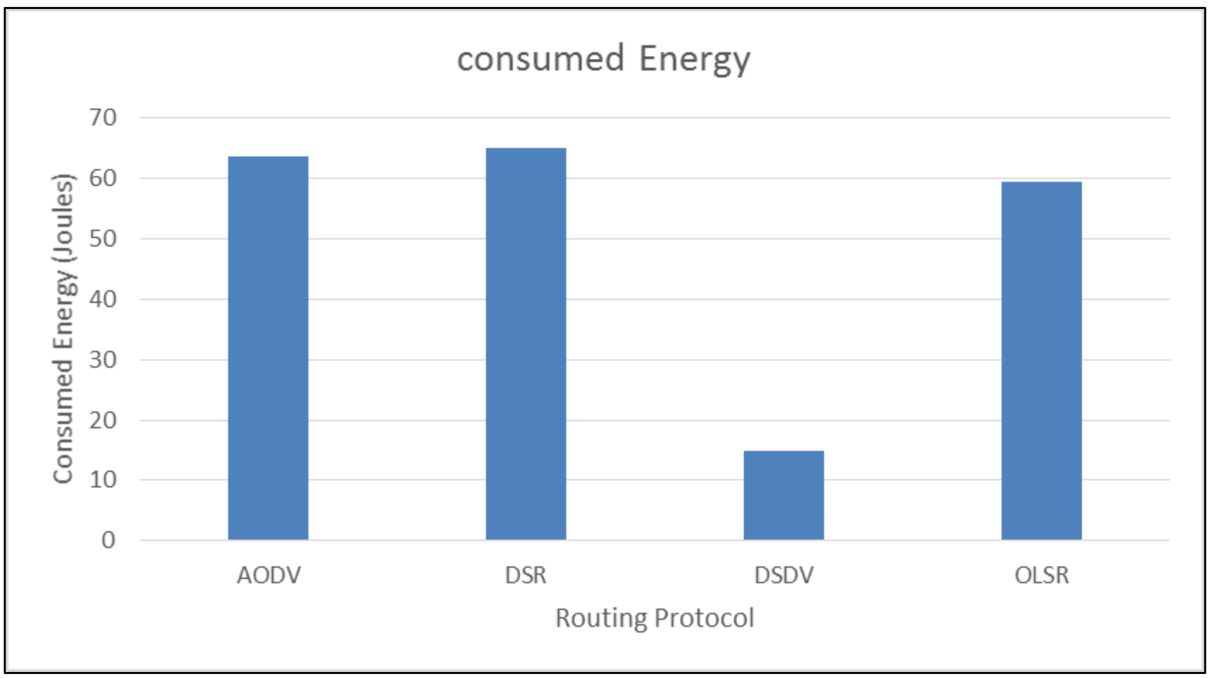


Figure 5. 12: total consumed energy for the entire network

In figure 5.12 we calculated the total energy consumed by the entire network for all 4 routing protocols for all nodes in the network, either participating in the routing process or not. Both ADOV and DSR routing protocols, we noticed that they consume a lot of energy, about

63.776 joules for AODV and 65.015 for DSR of which represent a high power consumption from a total of 110 joules the power of all nodes in the network. The protocol that consumes less power is the DSDV protocol with a total of 14.920 joules, the little power consumption of the DSDV protocol is due to the delay the protocol before it begins transmitting data packets, the time in which the nodes begins transmitting the data packets is small and hence the energy consumed is small. The last protocol, OLSR, consumes about 59.505 joules during the simulation time.

5.3.2 Network Lifetime

The entire network life time is the time that the source node is able to transfer data packets to its destination successfully. The process of sending data packets successfully requires valid routes between sender and receiver, the routes are the intermediate nodes that forwards data packets between the source and the destination. Successful data packets transfer requires that the intermediate nodes in these routes will continue to send data until the end of the transmission process. There are two obstacles that prevent the continuation of the transmission process. First, that these routes become invalid due to the movement of intermediate nodes due to its mobility, causing links breakages. And the other reason is due to power consumption and the depletion of nodes power.

In our experiment to evaluate network life time we used a scenario as shown in figure 5.13 below. The scenario consists of 50 nodes distributed randomly over a topography of 2000mX1000m. The transmission range of each node is 250m. Moreover, our scenario is static, where the nodes mobility is 0, because we only want to evaluate the effect of power consumption when using several routing protocol. We used one CBR flow to transmit data packets from source (node 0) to destination (node 1) as shown in figure 5.13.

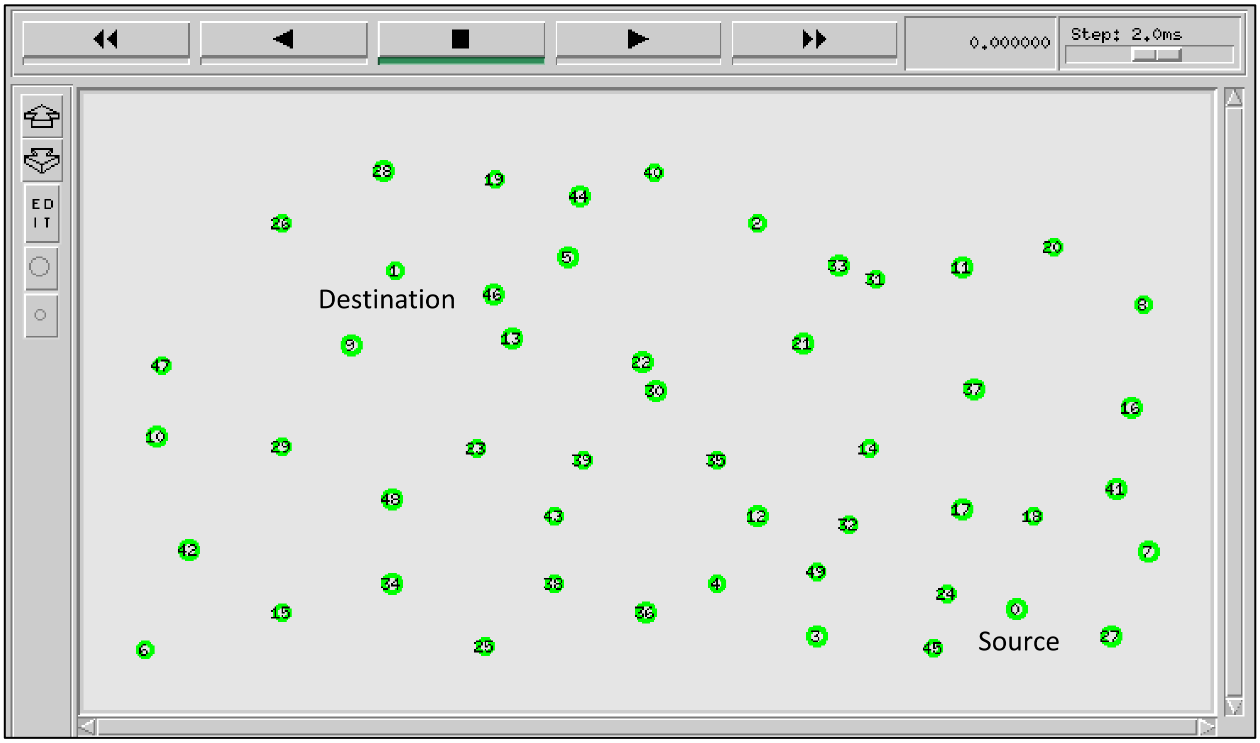


Figure 5. 13: simulation scenario for network lifetime test

Several routes are available from source to destination. As shown in figure 5.13, there are several valid paths between source and destination. What determines any of these routes will be used is the routing protocol (either AODV, DSR, DSDV or OLSR in our case). For example, the routing protocol could use path (0-24-49-12-35-22-13-1) to transfer data packets. Over time, and continuation of transmission process using the same path, the intermediate nodes will lose its energy and the path become invalid. The routing protocol will then searches for an alternate path, for example (0-17-14-21-2-40-19-1) and resumes the transmission. This process continues until all valid routes are exhausted. We calculate the time from the beginning of simulation until all valid paths are invalid, this period of time is called network lifetime. The complete parameters used in the simulation scenario are shown in table 5.4 below:

Table 5. 4: simulation parameters for network lifetime test

Simulator	NS-2.35
Channel	Wireless-Channel
Propagation	Two-Ray-Ground
Interface	Phy/WirelessPhy
Queue	DropTail/PriQueue
Queue length	50 packets
Antenna	Omni-Antenna
Protocols	AODV. DSR. DSDV. OLSR
simulation time	200 s
topography area	2000 X 1000 m^2
number of nodes	50 nodes
transmission range	250 m
Mobility	0 m/s
mac layer	IEEE 802.11
data payload	1024 bytes/packet
traffic type	CBR
# of flows	1 flow
Node Initial Energy	10 joules
Rx Power	0.2 W
Tx Power	0.9 W
Idle Power	0.01 W
Sleep Power	0.001 W

In the experiment we used the same parameters for each protocol separately, in order to measure the network lifetime. In figure 5.13 below, we calculated the network life time for each routing protocol. AODV and DSDV has the maximum network life time with about 88 seconds each. The protocol with the minimum lifetime value is DSR with about 69 seconds. While OLSR protocol has a value of about 83 seconds. This variation in values is due to the routing protocol nature and how it builds the routing paths. For example AODV Protocol is building routing paths upon request and does not need any routing tables, the paths that is built are saved for temporal use and may change at any time based on any topological change in the network. As a result, the routes used will change frequently, which means that a larger number of nodes will be involved in the transmission process and thus load distribution is relatively fair between nodes. With regard to protocol DSR, although it is a reactive protocol that works only upon request and minimizes overhead in the network, it has the minimum lifetime period, this is because the entire route in DSR routing mechanism is contained in packets header, which means larger packets and hence larger amount of energy consumed. DSDV is a table-driven routing protocol, the routing messages and overhead are distributed among all nodes in the network upon specific routines or triggered based on any change in the network topology, although routing overhead is higher than AODV protocol but it still able to prolong the network lifetime. This is simply because DSDV protocol runs in a static environment where all nodes are fixed in their position, and hence lower number of routing packets are needed (a total of 2204 routing packets for DSDV compared to 3763 routing packets for AODV). OLSR also consumes a lot of energy, this is because OLSR is proactive protocol and routing messages are flooded periodically in the network (mainly to select the MPR nodes and the messages sent from MPR to their neighbors). The total number of control messages sent in our example are (16773 routing packets) which consumes a lot of energy. Moreover, OLSR relay on specific nodes (called multipoint relay) that are selected by neighboring nodes, those nodes are responsible for facilitating flooding of control messages in the network. Reliance on specific nodes in the network leads to exhausting the relay nodes and hence shorten the network lifetime.

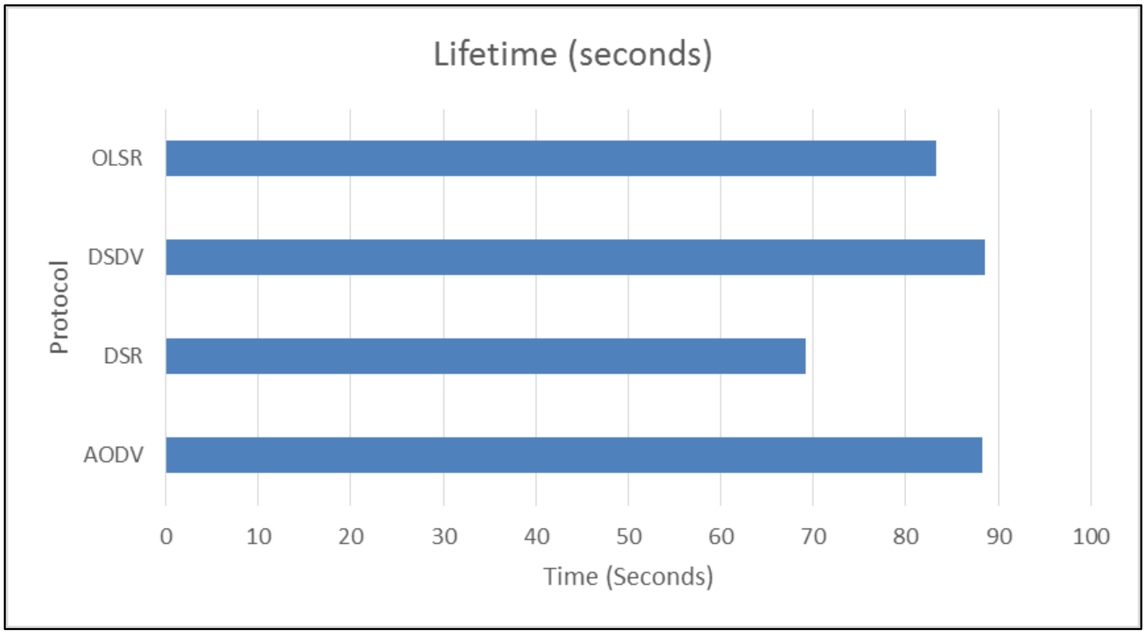


Figure 5. 14: network life time for all simulated routing protocols

Relying on specific nodes in the network for routing or facilitating control messages flooding could potentially shorten the network lifetime, this is the case in OLSR protocol as we explained before. The other routing protocols overcome this problem by distributing the control messages overhead over all of the nodes in the network like DSDV or AODV protocols. However, in some scenarios, routing protocol have to rely on a single node or group of nodes to send or receive from any source to any destination, this happens when there is not any other alternatives.in other words, that specific node is part of all available routes from source to destination and hence it will be used as an intermediate node when sending data packets despite the route used. For example, in our simulation scenario, in the left bottom corner, shown in figure 5.14 above, if node 25 wants to communicate with node 47, there are several available and valid routes (for example: “25-34-48-29-10-47” or “25-34-15-42-10-47” or “25-34-15-6-42-47” or “25-38-43-23-48-29-10-47” ….), all available routes from node 25 to node 47 do use node 10 as an intermediate node, this will consume node 10 and as a result shorten the network lifetime.

Exploitation of nodes in the network could lead to bad results, fair load distribution over all nodes in the network could potentially prolong the entire network life time and also prolong the individual nodes life and saves its energy for extra work. We can measure load balancing for each routing protocol by calculating the consumed energy variance among all nodes in the network shown in figure 5.15 below.

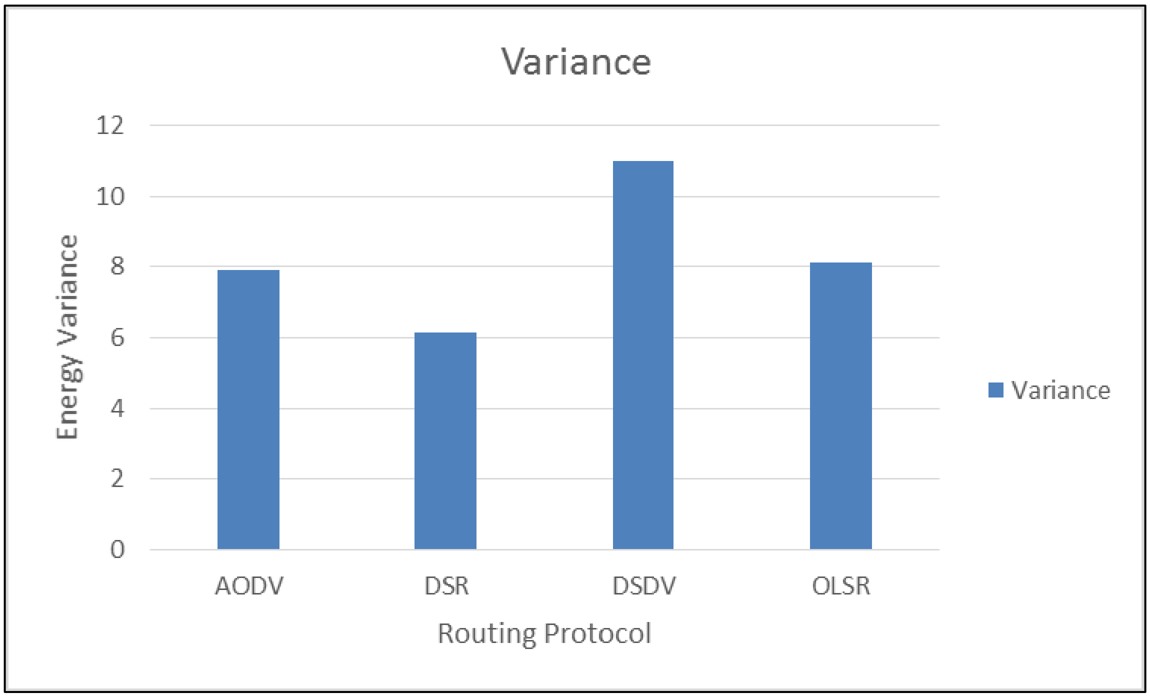


Figure 5. 15: energy variance for all tested routing protocols

The exploitation of specific nodes in the network affects the performance of the entire network, as we can view in figure 5.15, protocol DSDV has the highest variance value (11.00) which means unfair utilization of nodes in the network. Portion of the energy in DSDV protocol consumed by routing and overhead messages which distributed fairly among all nodes in the network, but the huge difference in nodes utilization is due to data packet routing process which is done by specific nodes, table 5.4 below shows the actual consumed energy by each routing protocol, as we noticed, few number of nodes consumed (only 9 nodes) at the end of network lifetime which means specific nodes are drained while others still have a high level of energy, also 40% of nodes consumed less than 50% of their initial energy. DSR protocol shows better results in energy consumption variance (6.15), although it is a high value but still better than other routing protocols in static environments, in table 5.5 below, DSR protocol drained 12 nodes, and only 14% of nodes consumed less than 50% of their initial energy. DSR also shows better load distribution results than AODV and OLSR, variance values are 7.88 for AODV and 8.10 for OLSR and also AODV and OLSR drained 16 nodes and 20% of nodes consumed less than 50% of their energy.

Table 5. 5: the complete power consumption for all nodes in the network

Node ID	AODV	DSR	DSDV	OLSR
2	10	9.598799	10	10
3	9.836126	10	5.245289	10
4	10	9.793858	4.836963	10
5	10	10	9.818338	10
6	0.988236	1.224438	0.332304	1.02461
7	4.872016	6.379042	4.625759	5.050621
8	2.685368	6.099881	3.340641	2.698397
9	8.168443	8.352652	4.458251	6.227347
10	2.004795	2.813061	0.389626	1.781367
11	7.457758	8.952578	8.84141	6.92235
12	10	9.219189	9.518006	10
13	10	8.250083	8.385851	9.692279
14	10	10	10	10
15	3.394779	3.895165	0.798147	3.191146
16	5.185152	7.779295	5.742974	5.969778
17	10	10	10	10
18	7.24277	10	6.655598	7.727765
19	8.689965	5.438862	7.830477	6.407437
20	4.196852	7.029288	4.844496	5.721555

21	9.799295	9.536209	10	10
22	10	8.83118	9.943982	10
23	10	9.197154	6.113066	9.413001
24	8.682457	8.937435	7.766463	8.349768
25	5.39627	5.153123	1.149773	4.630218
26	3.56875	2.704309	2.651343	2.99835
27	4.225018	5.702219	3.709452	4.645641
28	6.751683	3.697637	6.111179	4.751066
29	5.574673	7.079815	2.179577	4.586818
30	10	10	8.499544	10
31	7.049864	7.531503	8.097872	7.009505
32	10	10	9.398641	10
33	10	10	10	10
34	5.895072	5.7767	1.580785	5.106821
35	10	10	10	10
36	8.323089	7.401401	3.057795	8.11223
37	10	10	10	9.764315
38	8.043152	6.987551	2.758133	7.471424
39	9.556013	9.384751	6.504413	8.292556
40	9.982344	8.392797	10	10
41	6.244195	8.903255	6.17784	6.8311
42	1.998197	2.812389	0.378528	1.756413
43	7.910387	7.083327	4.07543	8.698459
44	10	7.038213	9.31308	7.952759
45	9.539459	10	5.7996	9.741423
46	10	10	10	10
47	1.834415	2.647503	0.517315	1.45735
48	7.425061	8.308161	2.598934	6.432389
49	9.378929	9.492753	7.026511	10
total	361.9006	367.4256	291.0734	350.4163

5.4 conclusions

The previous simulations shows a lot of variations in the performance of all routing protocols under specific conditions. We noticed that the density of the network is highly dependable on the scenario and the topological distribution of nodes over the network, and there is no relation between the performances of protocol under high dense or low dense networks, the topology and scenario affects the connectivity rather than the protocol itself.

The other parameter that affects the performance of routing protocol is the mobility of nodes. The speed of nodes affects all performance metrics we tested for all routing protocols, high speed networks suffer from high rate of links breakages, this issue affects the throughput, delay, overhead, and packet delivery fraction, for all reactive routing protocols, but in case of proactive protocols that uses periodical update of routing tables, the performance affected by these updates and shows constant behavior under low and high mobility conditions in case of overhead, but these protocols shows lower performance in throughput and packet delivery ratio as they are less aware of the topological changes in the network due to high mobility of nodes.

In power simulations, the network lifetime in proactive protocols is better in case of DSDV rather than OLSR, because DSDV distributes the load over more nodes rather than OLSR that relays on specific nodes to the entire work, which leads to shortening the entire network lifetime. In case of reactive protocols, the network lifetime is better in case of AODV rather than DSR. The AODV protocol maintains the routing information in routing tables while DSR maintains the full route in packets header and hence consuming more power to deliver these huge size packets. AODV and DSDV shows the same performance in network lifetime, but AODV protocol shows better results in fair utilization of nodes and distributes the load over the nodes rather than using specific nodes only.

Chapter 6: Enhancing the connectivity of Mobile Ad-hoc Networks by considering the Power and mobility of nodes

Finding the best routing path in the Mobile Ad-hoc Networks (MANETs) is a very critical issue when designing MANET routing protocols, since many conditions affects the connectivity of the network, one critical condition is nodes power; it affects the node availability and network connectivity, so that the power of overall nodes should be used wisely to keep the topology stable and durable as far as possible. Another condition is the node mobility as nodes of MANET are mobile for all the time, which causes to high rate of topology changes and link breakages. This also means high rate of overhead and routing messages flooded in the network.

In this chapter we propose a new routing algorithm that considers nodes power and mobility, in hope we prolong the network lifetime, and minimize the overall overhead in the network, and as a result enhancing the network connectivity.

6.1 Lowest cost and stable routes

The problem with MANET routing is to find the optimal path that satisfies our needs in prolonging the network lifetime and minimizing the overhead of the entire network, the traditional MANET routing protocols routing metric is the number of hops, that is, the routes are selected and stored in the routing table based on the number of intermediate nodes between the source and destination, optimal route is the route with minimum number of hops. Number of hops metric is very useful in minimizing the overall end-to-end delay. Minimizing end-to-end delay is desirable characteristic for MANET routing, but the problem is that traditional protocols like AODV, DSR, DSDV and OLSR works fine when mobility is 0 (static topology) or near 0, but on high mobile networks, these protocols fails to minimize the average delay as we noticed in the previous chapter. Also, MANET routing protocols does not take power metric into consideration, and hence the routing protocol may consume power of specific nodes, because it only considers the number of hops rather than the energy level of these intermediate nodes.

Nodes mobility and energy affects the network connectivity in terms of life time and delay. To enhance the performance of the routing protocol we need to consider the power of the nodes so as to prolong the lifetime of the network, this is done by balancing the load of the network and distribute routing work among nodes fairly. Topology change rate depends on the mobility of nodes, as we concluded in chapter 5, as the mobility increase the number of link breakages increase and as a result the total overhead increases significantly in case of reactive protocols and also the delivery ratio decrease.

Stability of routing paths is very important as it increases the connectivity of the network, to make routes more stable, we have to select them carefully based on mobility of the nodes. In dynamic topology, the nodes moves in random speeds in different directions, if a node moves in high speed, a link breakage probability will increase; the high speed mobile node will get out of reach quickly and causes a link breakage in the route it participates in. the routing protocol should be aware of nodes mobility and only selects routes with lower link breakage probability.

Moreover, the routing protocol should also be aware of the power of the nodes, and only selects routes with higher residual energy levels. This way the network lifetime will increase and routing work load will be distributed among larger number of nodes. The cost of routing will be reduced per each node, selecting the routes based on the minimum number of hops could potentially consumes specific nodes in the network and reduces the entire network lifetime.

Predicting the link breakage time could be done by calculating the speed of nodes for all intermediate nodes in any candidate route, the route with minimum speed factor will be selected as the optimal path from source to destination. Moreover, to distribute the work fairly among nodes and prolong the network lifetime, we need to select routes with higher residual energy, the residual energy of any route is the total residual energy for all intermediate nodes participating in that route.

6.2 power aware routing

Energy of nodes in the network is a very important resource and needs to be conserved to guarantee higher degree of connectivity and reliability in mobile ad-hoc networks. Calculating the routes residual energy is done using equation 6 below:

$$E_r(t) = \sum_{i=1}^{n} E_i(t) \qquad (6)$$

Where:

$E_r(t)$: is the total residual energy of any specific route r at any specific time t.

n: is the number of nodes in the route.

$E_i(t)$: is the residual energy of node i at any specific time t.

The optimal route is the route with higher level of residual energy E_r. Each node receives a route request message (RREQ) will store only the route with higher residual energy level and adds its own residual energy to the energy metric and forwards the message to its neighbors.

6.3 mobility aware routing

To make routes more stable and serve for longer period of time, mobility of intermediate nodes should be considered, the probability of link breakage degreases when selecting nodes with lower speeds to carry the routing burden, these nodes will remain in the transmission range of its neighbors for longer period of time and the route entry that uses that node will remain valid for longer time. We can predict the link lifetime by calculating the speed and distance between any specific node and its neighbors. It is better to select a node that will serve the process of routing for longer time and will not go outside the transmission range until the process completes. We can predict the time for a node to be in the range by calculating its speed and direction of movement. The speed and direction could be calculated by applying RSSI measurement for distance between two nodes (*i*, *j*). The Received Signal Strength Indicator (RSSI) describes the relation between transmitted powers and received powers in the following formula [48]:

$$p_r = p_t \left(\frac{1}{d}\right)^n \qquad (7)$$

Where p_r is receiving power, p_t is the transmitted power; d is the distance between sender and receiver nodes and n is the transmission factor whose value depends on the propagation environment.

Now we need to show the relation between RSSI and distance, for calculating the received power based on this model, we first calculate the received power at a reference distance using the Friis formula (given in Eq. (7)). Then, we incorporate the effect of path loss exponent and shadowing parameters [49].

$$RSSI = -(10 * \log_{10}(d_{i,j}) - A) \qquad (8)$$

The theoretical distance between nodes is given by:

$$d_{i,j} = 10^{\frac{RSSI-A}{-10*n}} \qquad (9)$$

Where:

d_{ij}: distance from node I to node j.

RSSI: receiving signal strength indicator.

A: is received power from reference distance which is 1 meter

n: is the transmission factor whose value depends on the propagation environment.

By using Eq. (9) each node knows exactly the distance to all its neighbors and hence decides which node to use as the next hop route. By sending several signals to measure distance over a specific period of time will give an estimated information about node movement and speed. For example, if we send several RSSI check and calculated the distances between *i* and *j* we can retrieve the speed and whether the node *j* moves closer or moves away from node *i*. figure (6.1) shows an example of two mobile nodes *i, j*.

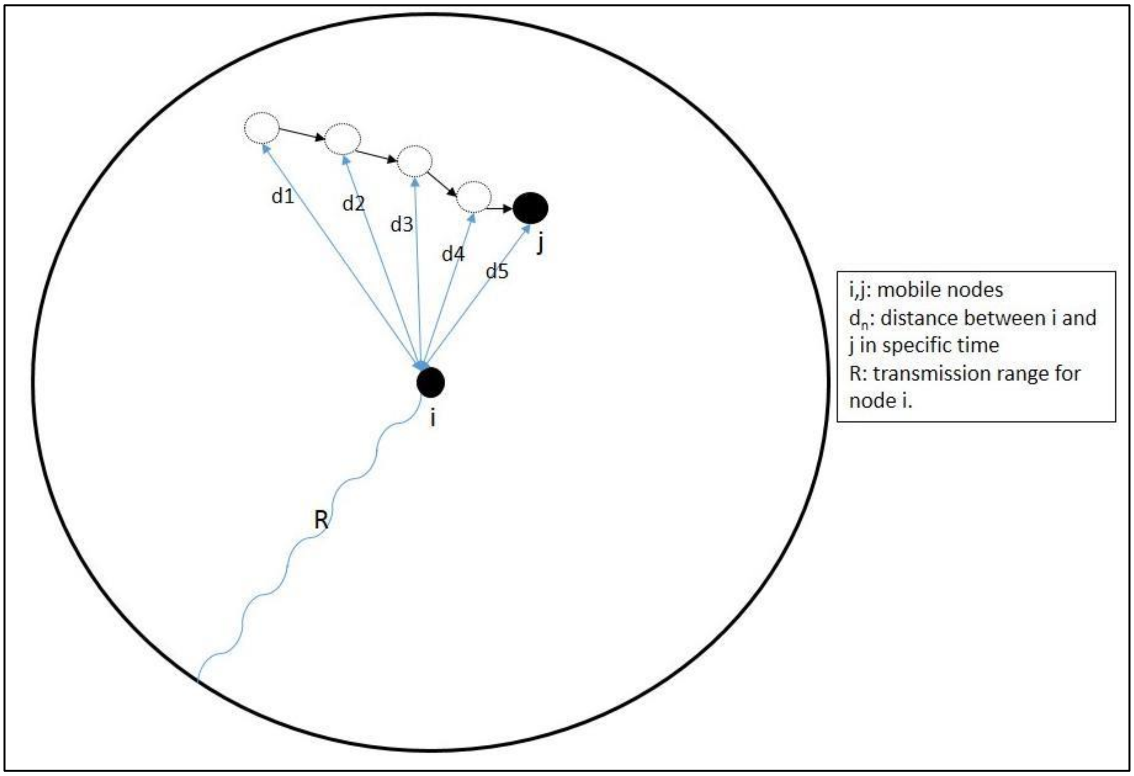


Figure 6. 1: Estimating speed and direction using several RSSI signals

In figure 6.1, Node i can calculate the speed of node j by sending several RSSI request and measure the distances over a specific period of time t; to check the speed and direction of movement as follows:

$$NS = \frac{\sum_{k}^{n}\frac{|d_{k+1} - d_k|}{t_k}}{n} \qquad (10)$$

Eq. (10) shows the average node speed (NS) of node *j* in reference to node *i*, *where* | $d_{(k+1)}$ - d_k | is the distance that node j moves after each successive measure *k* and t_k is the time between every successive measure, *n* is the number of times we check the distance between *i* and *j*. Now, we need to check whether node *j* moves away from node *i* or moving toward node *i*;

this could be calculated by the difference between d_n and d_1 ; if the difference is positive then the node is coming closer and if negative then the node moves away. When the node moves away we predict that the node *j* will be out of range after *LBT(i,j)* time as follows:

$$LBT(ij) = \frac{R \pm d}{NS} \qquad (11)$$

Where:

LBT(ij): is the estimated link breakage time between nodes *i* and *j*.

d: distance between *i* and *j*.

R: transmission range.

The *LBT(i,j)* shows the time that anode still be reachable based on its mobility and direction of movement; in other words the link between *i* and *j* will break after *LBT* time.

6.4 Scheme and optimal route calculation

We selected AODV protocol to be the base protocol for our implementation, as it shows better performance than DSR reactive protocol for all performance metrics studied in chapter 5.

The AODV protocol selects optimal route based on the number of hops, the optimal path is the path with minimum number of hops, and the mechanism for selecting a route goes as follows: each node receives a RREQ message checks its own routing table for a valid entry for the desired destination, if it founds a valid entry with fresh sequence number it will reply with a RREP message using the previous hop node to inform the source node that it has a valid route for the destination, if no valid route found the node will forward the RREQ message to its neighbors and incrementing the hop count metric by one.

In our model, we terminated the hop count metric and instead we used the residual energy and link breakage time, those two metrics are stored as an optimal route metric. The complete scheme for building and storing routes goes as follows:

- The process starts from any node that wants to communicate with any other node in the network. The sending node is called the source node and the target node is called the destination node. The source node generates a route request message RREQ containing the source node IP address and the destination IP address, sequence number for source node, sequence number for destination, and broadcast id. This RREQ message is broadcasted to all neighbors.
- Any neighbor node receives the RREQ message will first check whether it is the destination node or not, if it is the destination node it will respond with a route reply message to the destination holding the entire route information. And if it is not the destination, the node will check its neighbors by sending several RSSI signals to sense their mobility status and determines the speed and direction for each neighbor node, then it will add its own energy level (E) and the estimated link breakage time (LBT) for each neighbor node to the optimal route metric field in the route request message. The neighbor node that receives that RREQ message will store the two values in its routing table. If that neighbor node receives another RREQ message containing the same destination, it will calculate the optimal route metrics as follows:

$$ORM_r = E_r * LBT_r \qquad (12)$$

Where:

ORM_r: is the optimal route metric for any specific route *r*

The node will calculate ORM for the new coming RREQ message and compare it with the route entry in its own routing table, if the new ORM is greater than the old stored ORM it will replace the entry with the new one.

- That neighbor node also repeats the previous operation by sensing its neighbor's mobility status, then it adds up its own energy and LBT to the RREQ message and forwards it to each neighbor node.
- The RREQ message propagates until it reaches the desired destination, the destination node receives RREQ message will generate a route reply message RREP and sends it back to the source using the stored routing entries in the intermediate node.
- The RREP message will propagate to the source using the reverse route, the source node then receives the RREP message and starts sending data using the optimal route metric stored in its routing table.

To further illustrate the routing process we will use the following example shown in figure 6.2 below:

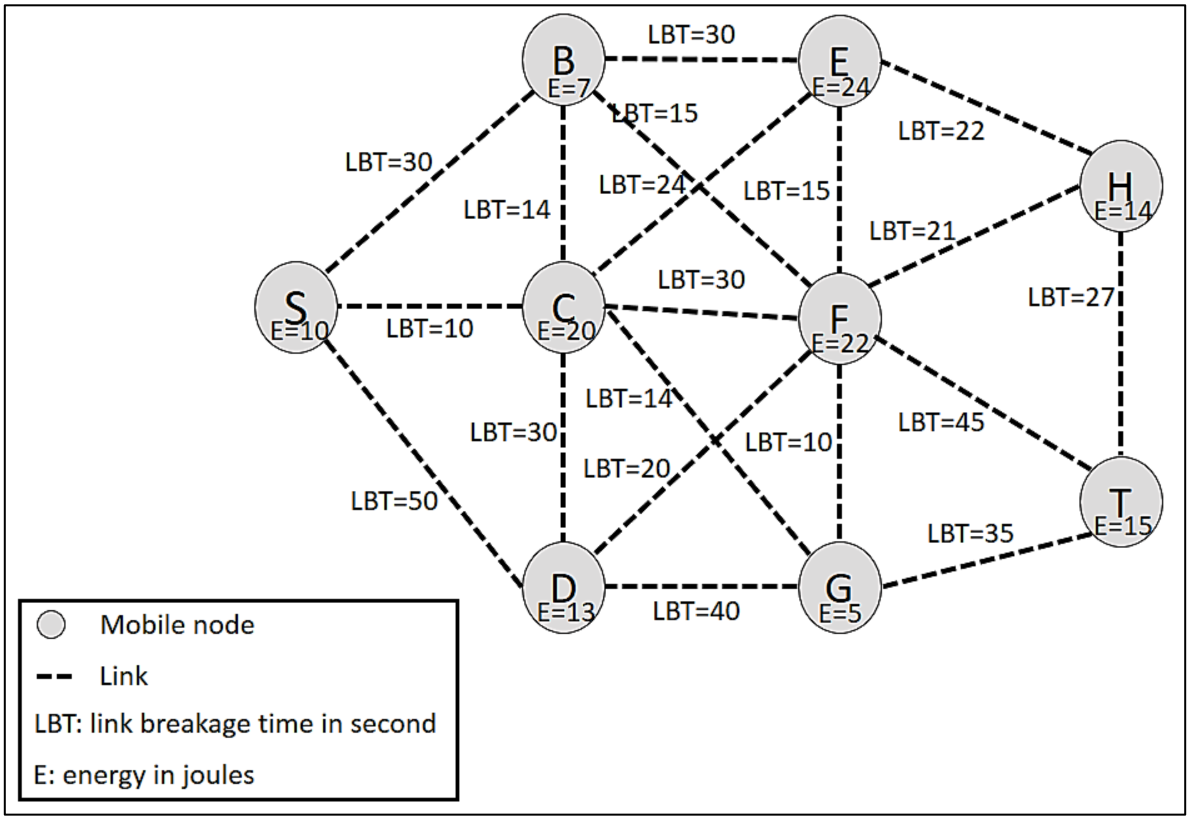


Figure 6. 2: Example of routing mechanism

The example shows a scenario of 9 mobile nodes, consider that node S wants to communicate with node T, the following will occur:

1- Node S will first sense its neighbors (neighbors of S are B, C, D) by sending several RSSI signals, the speed and direction of each neighbor node will be recognized, then S will generate a RREQ message holding the energy value of S and link breakage time between S and the concerned node, in addition to source address and destination address.

2- Nodes B, C and D will receive the route request message and record the following entries in their routing tables:

Routing table for node B			
Destination	Next hop	LBT	Energy
S	S	14	10

Routing table for node C			
Destination	Next hop	LBT	Energy
S	S	10	10

Routing table for node D			
Destination	Next hop	LBT	Energy
S	S	50	10

3- Nodes B, C, and D will also sense their neighbors and send RREQ messages for their neighbors after calculating the LBT values for all neighbors. Node B will send the total energy (energy for node S and its own energy) and also the LBT to that concerned neighbor. Neighbors of B for example: C, E, F and S will receive the RREQ message holding the total energy and the lowest LBT value to source node S .Node E will store the following entries in its routing table after receiving a route request from node B:

Routing table for node E after receiving RREQ from node B			
Destination	Next hop	LBT	Energy
S	B	30	17

After that node E will receive the same RREQ from node C asking for the destination, the RREQ from C holds the following values: LBT=10 and E=30. Node E will calculate the ORM in its routing table and for the new coming request.

ORM for the RREQ=10*30 =300

ORM for the routing table entry=30*17=510.

Node E will keep the routing entry for that destination as the ORM value is greater than the new coming one.

Now let's see what happens in node F, node F will receive a RREQ from node B and the following information will be stored

Routing table for node F after receiving RREQ from Node B			
Destination	Next hop	LBT	Energy
S	B	24	17

Node F will also receive route request from node C, and the LBT=10 and the E=30. Node F will calculate the ORM for that RREQ, ORM=30*10=300. And calculates the ORM for the route entry in the table, ORM=24*17=408. Node F will keep the value in the routing table.

Finally node F will receive a RREQ from node D, the message holds the following information: LBT=20, E=23, then the ORM for the message =20*23= 460. Node F will replace the route entry with the following values:

Routing table for node F after receiving RREQ from node D			
Destination	Next hop	LBT	Energy
S	D	20	23

Node G also receives a RREQ message from nodes C and D, the ORM from node C will be: 10*30=300, and ORM from D will be: 40*23=920. The routing table for node G will be:

Routing table for node G			
Destination	Next hop	LBT	Energy
S	D	40	23

Node H will also receive RREQ from nodes E and F, the ORM from E will be: LBT=22, and E=41, ORM=22*41=902. And the RREQ from node F holds: LBT=20, E=45, ORM=20*45=900. The routing table for node H will store the following:

Routing table for node H			
Destination	Next hop	LBT	Energy
S	E	22	41

Finally, node T will receive RREQ messages from node H, F, and G. message from H hold the following information: LBT=22, E=55, the ORM value=22*55=1210. The message from F holds the following information: LBT=20, E=45, the ORM =20*45=900. And finally, message from G holds the following information: LBT=35, E=28, the ORM value=35*28=980. Node D will store the following information:

Routing table for node T			
Destination	Next hop	LBT	Energy
S	H	22	55

Node T is the destination node, it will generate a RREP message and will unicast it to the source using the information stored in its routing table. The RREP message will be sent to node H and node H will add a new entry in its routing table holding the information from T. the final routing table for node H will look like this:

Routing table for node H after receiving RREP from T			
Destination	Next hop	LBT	Energy
S	E	22	41
T	T	27	15

Node H in turn forward the RREP message to next hop in its routing table which is node E, and a new route entry is stored. The final routing table for node E will be:

Routing table for node E after receiving RREP from H			
Destination	Next hop	LBT	Energy
S	B	30	17
T	H	22	29

Node E will unicast the message for node B and holding the route information and a new entry will be stored in the routing table:

Routing table for node B after receiving RREP from E			
Destination	Next hop	LBT	Energy
S	S	14	10
T	E	22	53

Finally node S receives a RREP message and updates its routing table, then node S will start sending data using these information. The final routing table for node S:

Routing table for node S after receiving RREP from B			
Destination	Next hop	LBT	Energy
T	B	22	60

The routing tables will remain unchanged and will be used for further routing processes for other nodes until one of the following occurs:

1- A link breakage occurs due to nodes mobility or some intermediate node consumes all of its energy. In that case the node trying to send data using a broken link will generate a route error message RERR and broadcast this error message to its neighbor informing them that it has no more valid route to that node, and delete that routing entry from its routing table. The source node after receiving the RERR message wil generate another RREQ message to look for an alternate route.
2- The route entry expires after specific period of time, this will help routing protocol to be aware of changes in the network topology

All the information collected from a single RREQ message as shown in the previous example are useful and kept for further use. Suppose that node C wants to communicate with node H, it will send a RREQ to its neighbors B, E and F, node B will respond with RREP message to inform C that it has a valid path to H with the following information: LBT= 22, E=53, and node E will respond with RREP with the following information: LBT=22, E=29, while F will send RREQ to H and waits for RREP. Node C stores the following information:

Routing table for node C after receiving RREP from B			
Destination	Next hop	LBT	Energy
T	B	22	53

Node C will start sending data using these information, when a RREP received from node F, it will compare the ORM and stores and uses the larger one.

6.5 Simulation and Results

In this section we will simulate our new model and compare our results with other routing protocols in terms of network life time, load distribution and overhead and other performance metrics. We will use the same scenario and parameters used in section (5.3.2) table (5.2) for network lifetime simulations, and the same scenario and parameters used in section (5.2) for mobility simulations. First we will compare the new enhanced AODV (EAODV) algorithm with the previous results we concluded in section (5.3.2) table (5.1).

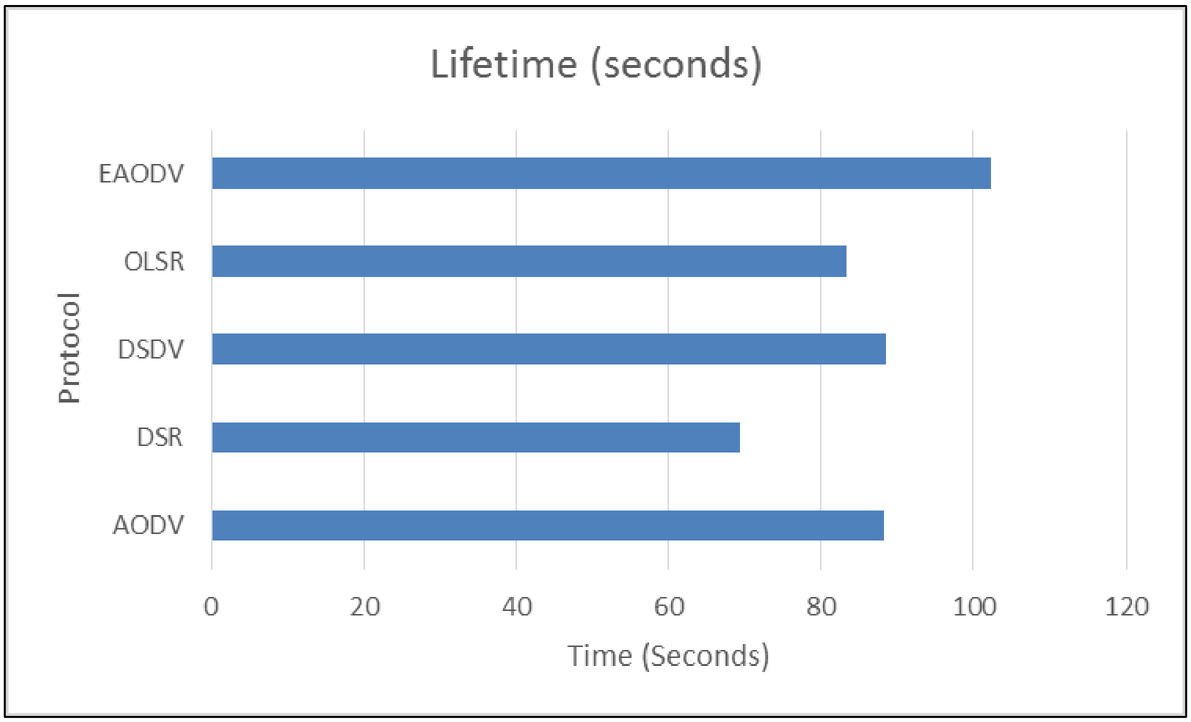


Figure 6. 3: Enhanced AODV network lifetime compared to other protocols

Figure 6.3 shows the network lifetime for the enhanced AODV protocol, we notice that considering the energy level of nodes is very important in prolonging the network life time, when comparing the ordinary AODV protocol, the lifetime of AODV is about 88 seconds, and for EAODV algorithm, the lifetime is extended to about 102 seconds, about (27%) longer than ordinary AODV. And also about (27%) better than DSDV proactive protocol.

Prolonging the network lifetime is a result of fair utilization of nodes in the network, the algorithm does not rely on specific nodes only because these nodes provides the minimum number of hops that AODV, DSR, OLSR, and DSDV implements, but instead the algorithm uses nodes in the network wisely and selects the optimal routes based on the energy level of intermediate nodes in routes.

Fair load distribution over all nodes can help in enhancing the entire network life time, figure 6.4 shows the consumed energy variance for EAODV. The results shows that EAODV do better in terms of load distribution, and utilizing more nodes.

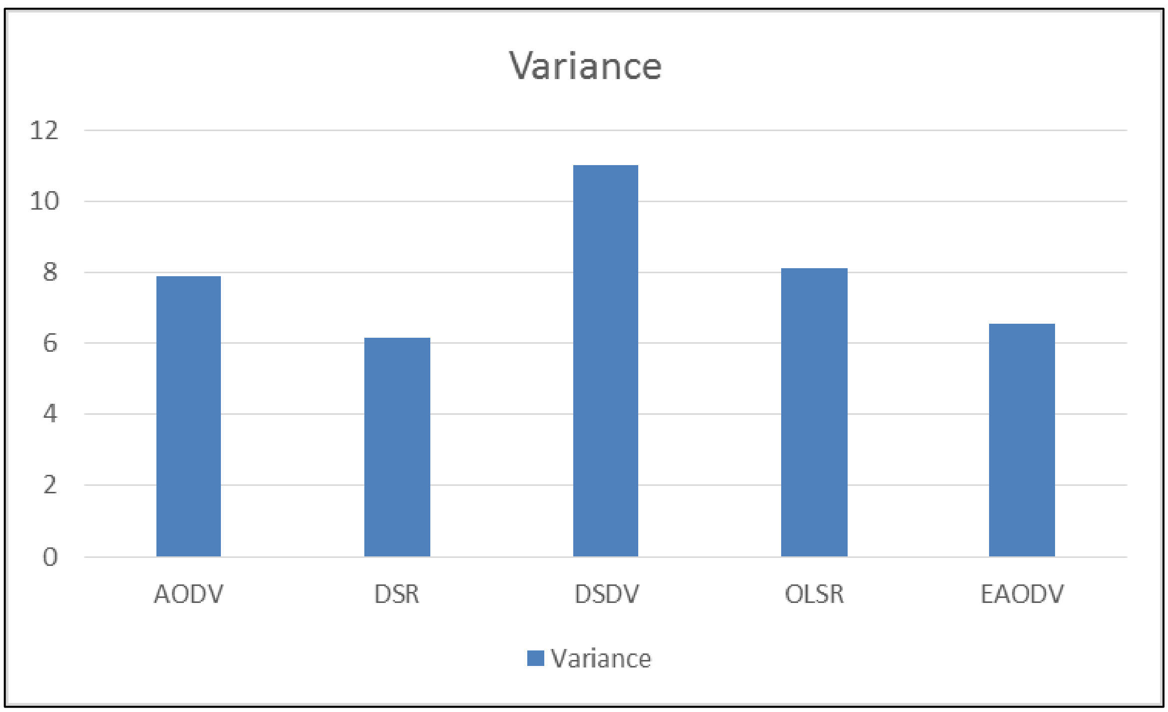


Figure 6. 4: consumed energy variance for EAODV compared to other protocols

The EAODV has drained 26 of the nodes in the network compared to 16 nodes become out of energy in the ordinary AODV, this means that EAODV used more nodes to complete the routing mission, not only relying on specific nodes in the network. Table 6.1 below shows the complete consumed energy for all nodes in the network for all routing protocols.

Table 6. 1: Energy consumed for all nodes in the network for all routing protocols

Node ID	AODV	DSR	DSDV	OLSR	EAODV
2	10	9.598799	10	10	10
3	9.836126	10	5.245289	10	10
4	10	9.793858	4.836963	10	10
5	10	10	9.818338	10	10
6	0.988236	1.224438	0.332304	1.02461	0.962149
7	4.872016	6.379042	4.625759	5.050621	6.790134
8	2.685368	6.099881	3.340641	2.698397	8.03061
9	8.168443	8.352652	4.458251	6.227347	9.528756
10	2.004795	2.813061	0.389626	1.781367	2.040674
11	7.457758	8.952578	8.84141	6.92235	9.017765
12	10	9.219189	9.518006	10	10
13	10	8.250083	8.385851	9.692279	10
14	10	10	10	10	10
15	3.394779	3.895165	0.798147	3.191146	4.052386
16	5.185152	7.779295	5.742974	5.969778	7.499513
17	10	10	10	10	10
18	7.24277	10	6.655598	7.727765	9.75653
19	8.689965	5.438862	7.830477	6.407437	9.671764
20	4.196852	7.029288	4.844496	5.721555	6.336406
21	9.799295	9.536209	10	10	10
22	10	8.83118	9.943982	10	10
23	10	9.197154	6.113066	9.413001	10
24	8.682457	8.937435	7.766463	8.349768	10
25	5.39627	5.153123	1.149773	4.630218	6.924485
26	3.56875	2.704309	2.651343	2.99835	4.208818
27	4.225018	5.702219	3.709452	4.645641	6.068553
28	6.751683	3.697637	6.111179	4.751066	7.380887
29	5.574673	7.079815	2.179577	4.586818	6.710235
30	10	10	8.499544	10	10

31	7.049864	7.531503	8.097872	7.009505	7.974053
32	10	10	9.398641	10	10
33	10	10	10	10	10
34	5.895072	5.7767	1.580785	5.106821	7.353952
35	10	10	10	10	10
36	8.323089	7.401401	3.057795	8.11223	10
37	10	10	10	9.764315	10
38	8.043152	6.987551	2.758133	7.471424	10
39	9.556013	9.384751	6.504413	8.292556	10
40	9.982344	8.392797	10	10	10
41	6.244195	8.903255	6.17784	6.8311	8.910274
42	1.998197	2.812389	0.378528	1.756413	2.007112
43	7.910387	7.083327	4.07543	8.698459	10
44	10	7.038213	9.31308	7.952759	10
45	9.539459	10	5.7996	9.741423	10
46	10	10	10	10	10
47	1.834415	2.647503	0.517315	1.45735	1.959212
48	7.425061	8.308161	2.598934	6.432389	9.374478
49	9.378929	9.492753	7.026511	10	10
Total	361.9006	367.4256	291.0734	350.4163	402.5587

The table shows that more nodes participated in the routing process which leads to prolonging the entire network lifetime. Moreover about 87.5% of the nodes has consumed more than 50% of its energy and only 12.5% of intermediate nodes remains with more than half charged, this again indicates that the EAODV algorithm utilizes most of the intermediate nodes.

Now we will analyze the mobility simulation results for the EAODV algorithm, we used the scenario in section 5.2 to compare the results.

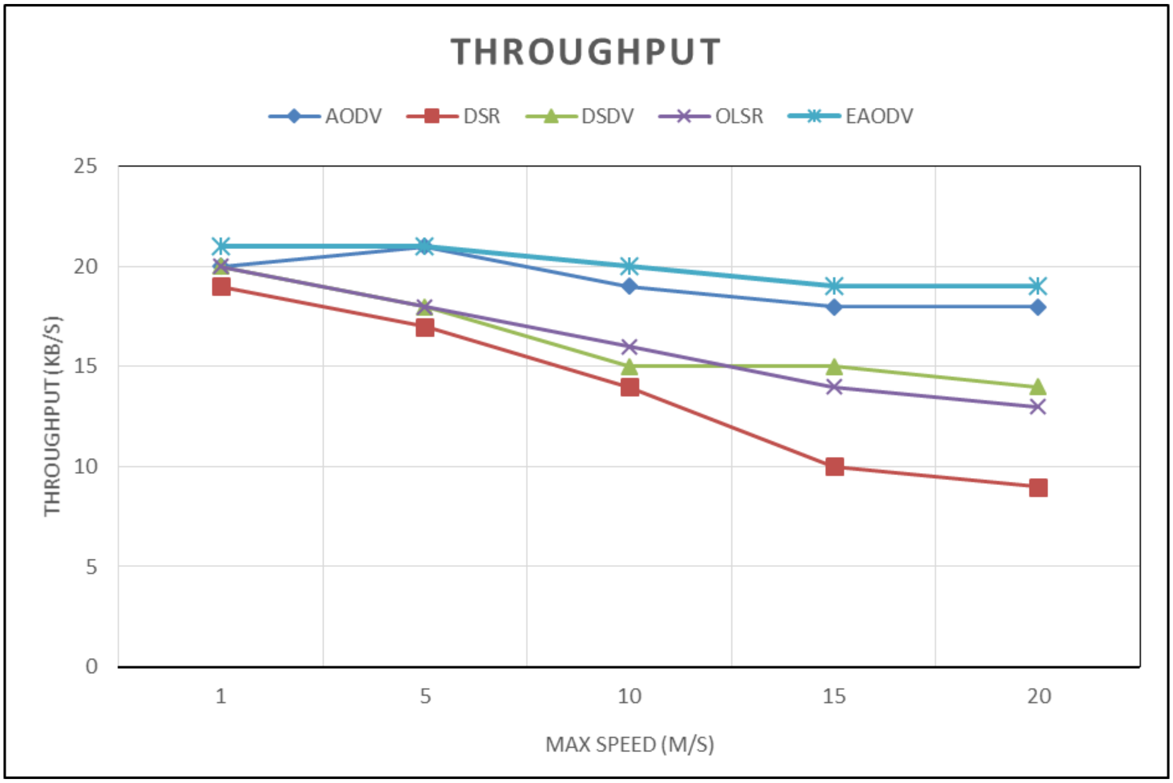


Figure 6. 5: throughput for EAODV compared to other routing protocols

The throughput shown in figure 6.5 of the entire network enhanced by little fraction compared to ordinary AODV and even better than all other routing protocols even on high dynamic network, this due to routes stability and the algorithm selects routes with higher estimated link breakage time, this leads more data to be successfully delivered to destinations before any link breakage occurs, especially for long routes with higher number of routes being used.

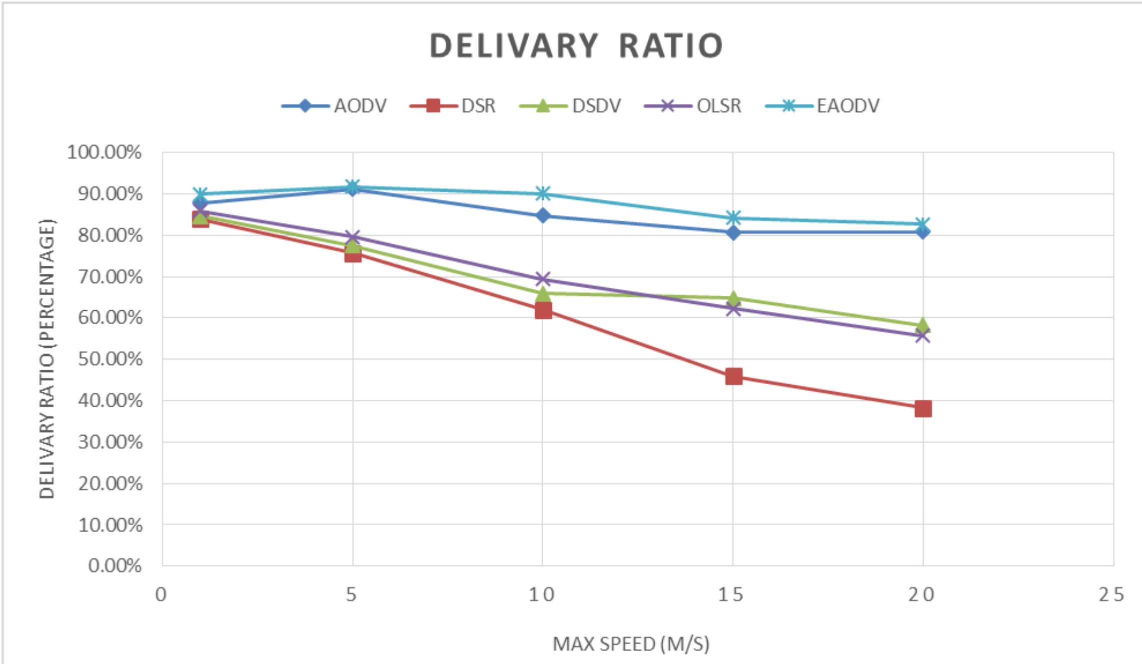
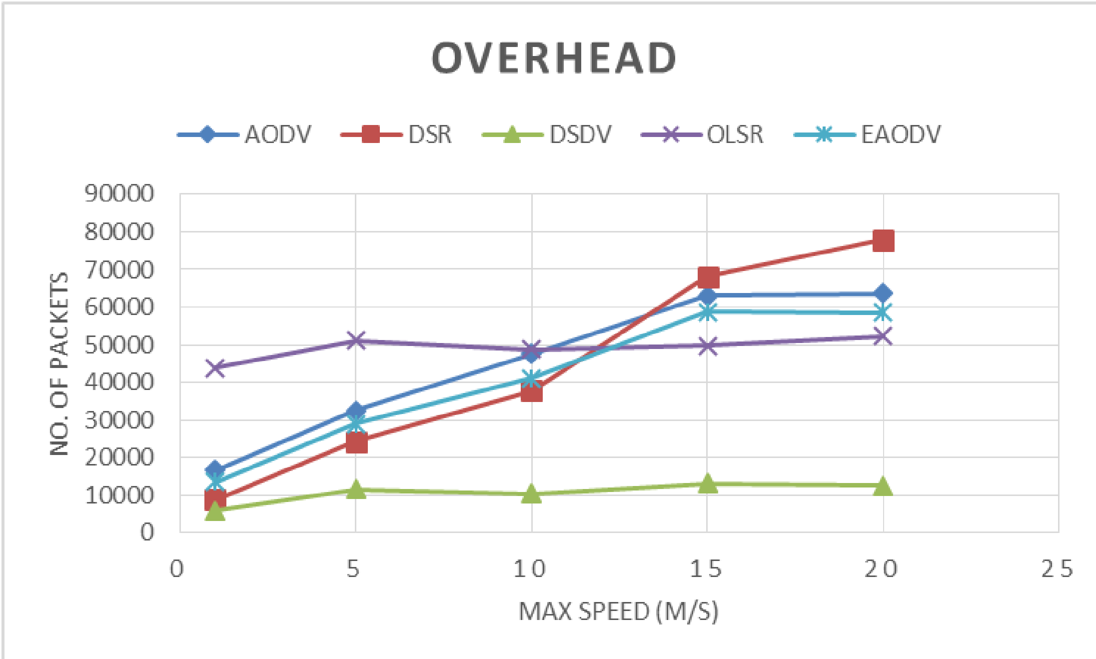


Figure 6. 6: Packet Delivery Fraction for EAODV compared to other routing protocols

The packet delivery fraction also enhanced because of optimizing the routes used by their mobility stability rather than the number of hops used. The algorithm will result in higher delivery of generated packets by sources and minimizes the total number of dropped packets due to mobility of nodes and high rate of link breakages.



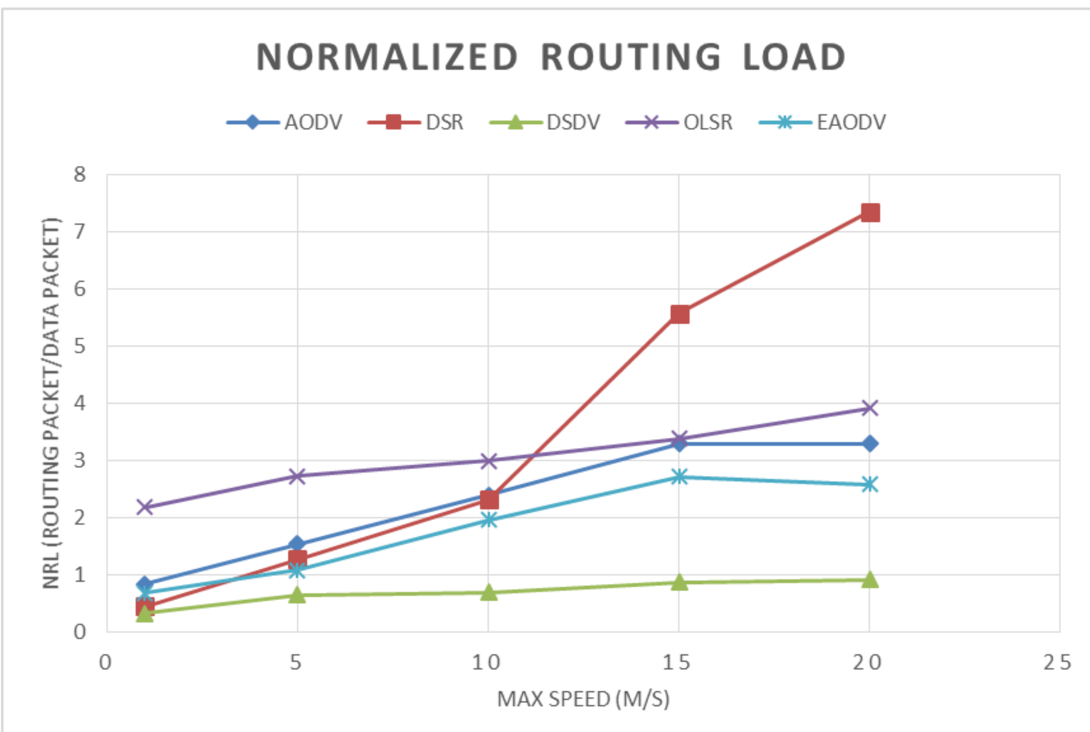


Figure 6. 7: Overhead and NRL of EAODV compared to other routing protocols

The overhead shown in figure 6.7 shows the exact amount of routing data needed to deliver one data packet, and also the total number of routing packets needed for EAODV protocol compared to all other routing protocols under all mobility conditions.

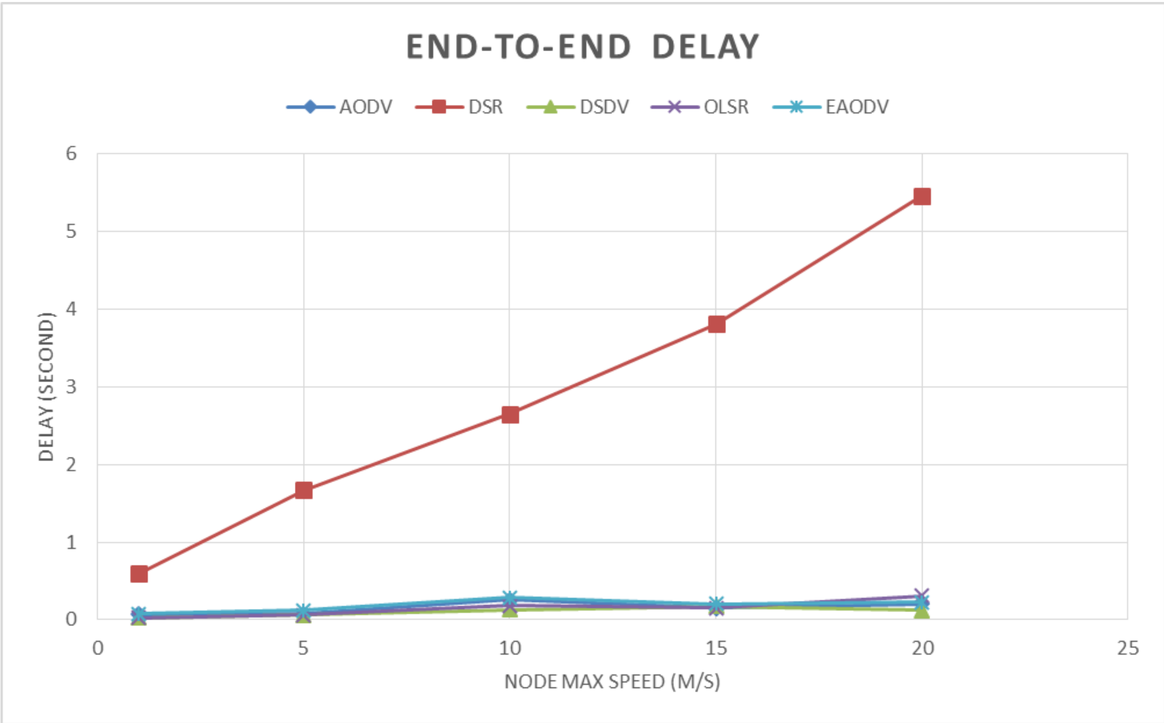


Figure 6. 8: End-to-End delay for EAODV compared to all other routing protocols

All of the results are promising except for the delay shown in figure 6.8, we were expecting this withdraw because of longer routes being used, and the ordinary AODV uses the shortest paths (i.e. the minimum number of hops) to deliver data. While in our algorithm, the EAODV uses the routes with higher level of stability based on their mobility status, preferred links are the links with longer estimated breakage time, and these routes may use larger number of hops, and as a result increasing the total average end to end delay. Although the delay is lower than ordinary AODV but it still acceptable, and the advantaged we get from EAODV covers this minor withdraw.

Table 6. 2: performance values for all routing protocols vs. EAODV

		Routing Protocol					Enhancement (EAODV vs. AODV)
		AODV	DSR	DSDV	OLSR	EAODV	
Performance Metrics	Throughput (KB)	19.2	13.8	16.4	16.2	20.2	+5.22%
	End-to-End Delay (second)	0.1516	2.8362	0.1035	0.1455	0.1841	-21.43%
	Packet Delivery Fraction (%)	85.03%	61.14%	70.17%	70.56%	88.04%	+3.5%
	Routing Overhead (Packet)	44770	43359.2	10742	49161.4	40231.6	+10.13%
	Normalized Routing Load (routing/data packets)	2.2641	3.3849	0.6801	3.0336	1.7992	+20.5%
	Consumed Energy Variance (joule)	7.8857	6.1556	11.0019	8.1016	6.5540	+16.88%
	Network Lifetime (second)	88.23	69.25	88.57	83.35	102.17	+15.79%

Table 6.2 above shows the final performance metrics for all tested routing protocols compared to our own protocol (EAOV). We notice that AODV results are the best in terms of throughput, delivery fraction and network lifetime. Our own model (EAODV) shows better results than ordinary AODV for all performance metrics except for end-to-end delay. The values shown are the average values for all different scenarios including all speeds. For example, the throughput shown for AODV is the average throughput for all tested scenarios for AODV on different speeds. The last column in the table shows the average enhancement that our model achieved compared to ordinary AODV protocol. For example EAODV achieved 5.22% higher throughput compared to AODV and over 20% better Normalized routing load (minimizing routing load), the major withdraw with our model is the average delay where the delay increases by about 21%. From this table we notice that applying mobility and energy aware mechanisms potentially increases the performance metrics for the routing protocol.

To further analyze the performance of the selected routing protocol compared to our approach (EAODV) we will study the correlation between several performance parameters and how these metrics affects each other. Before we begin, the results shown in the next lines are made using 5 different scenarios for each routing protocol including our own protocol (EAODV), these five different scenarios are applied to all routing protocols to maintain the results.

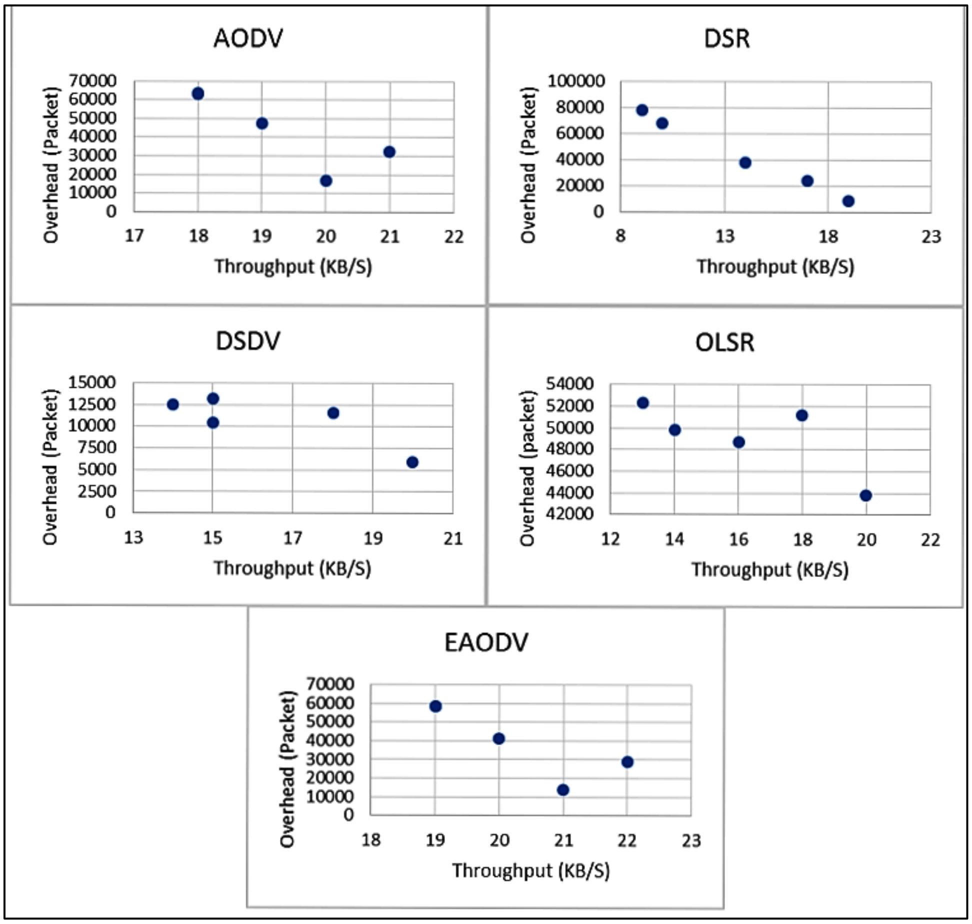


Figure 6. 9: Throughput vs Overhead

Figure 6.3 shows the relation between the average throughput and the total overhead for all tested routing protocols. We notice that the higher the throughput is the minimum the number of routing packets used. This is true because the higher the number of routing packets (overhead) means that the routing protocol detects more links failures and needs to maintain new routes by sending more routing packets to search for alternate routes. This situation results in higher delays and greater amounts of data packets are dropped due to link failures, hence the total throughput is decreased. Also we notice that all routing protocols shows the same effect for all tested scenarios.

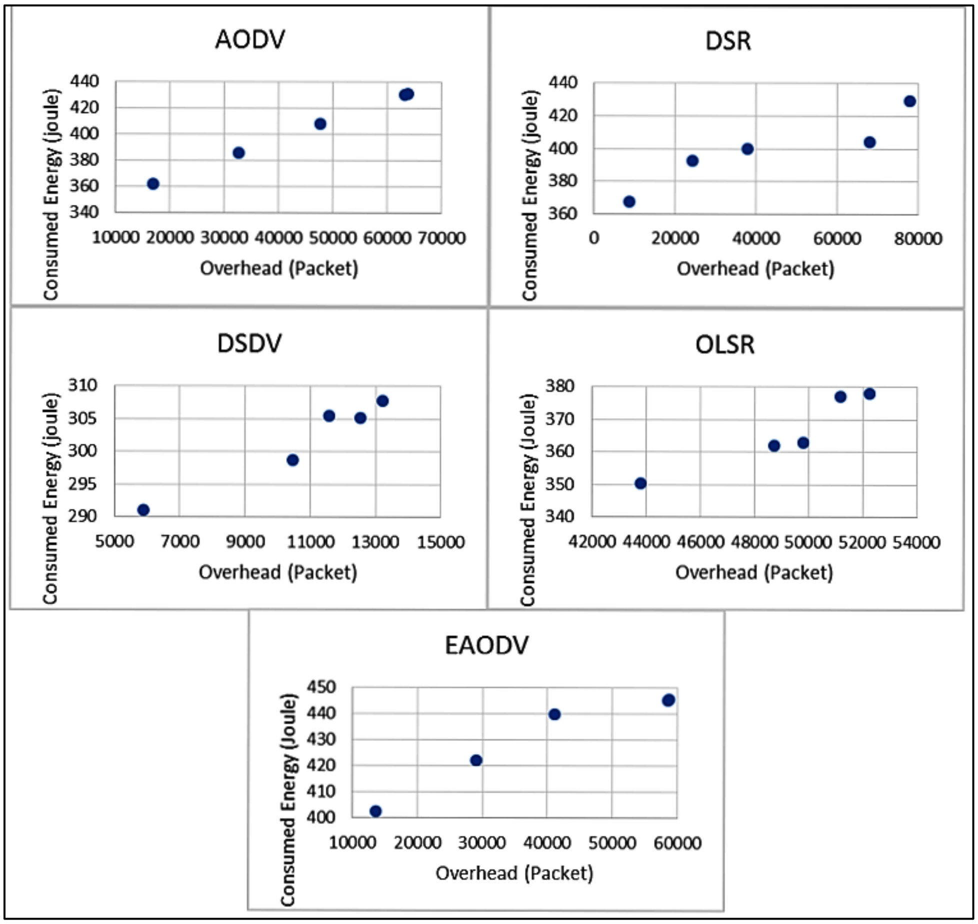


Figure 6. 10: Overhead vs. total consumed energy

Overhead also affects the total incurred energy in the network as shown in figure 6.4. The total consumed energy of the entire network represents the amount of power that all nodes in the network have consumed throughout the simulation time. This value increases as the total number of routing packets (overhead) increases, as we discussed in section 4.1.2 and section 4.2.4 the energy consumed depends on the number of packets being received or transmitted at each node, hence any increase in the total overhead will increase the total incurred energy of the entire network. This relation between overhead and consumed energy is the same for all routing protocols.

Delay is very important metric in MANET and its undesired in real time applications, in figure 6.5 below we studied the relation between the delay and average throughput. We notice that a higher throughput means minimum delays, and this is true because the delivery of higher amounts of data per unit of time requires minimum delay time at nodes level and at routing protocol level.

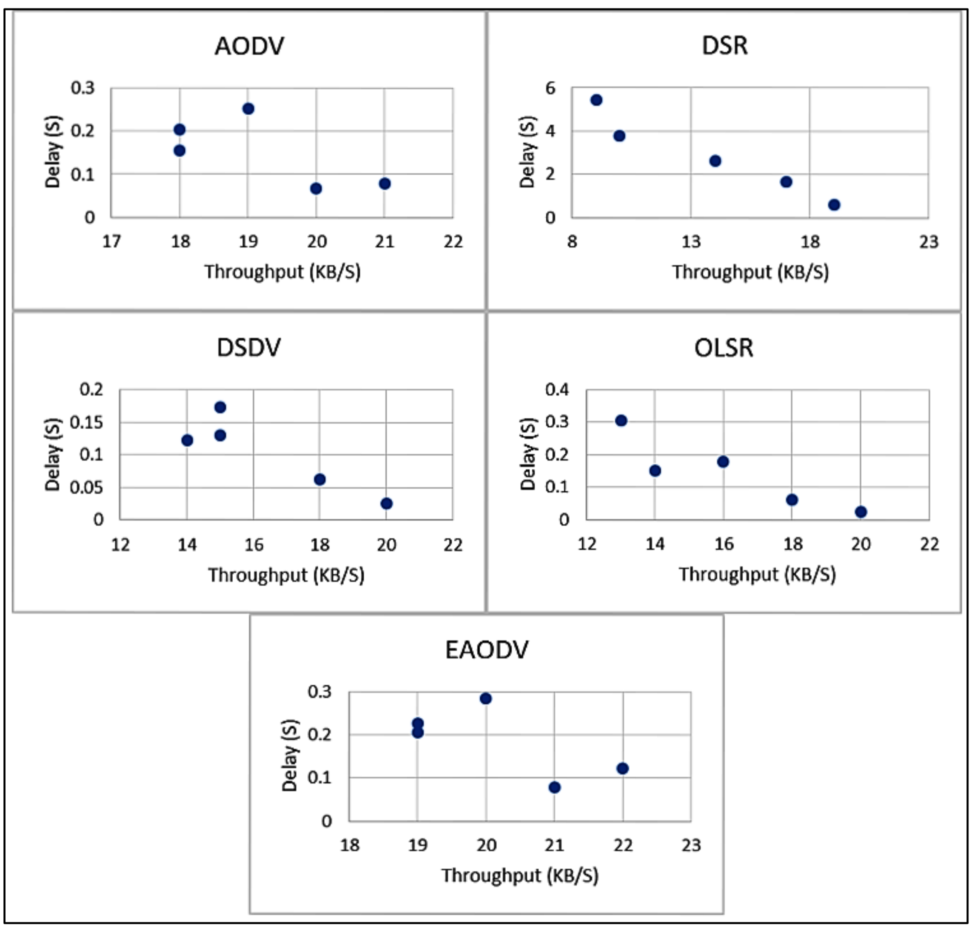


Figure 6. 11: Delay vs. Throughput

The routing protocol plays a role in such correlation because it determines the number of hops to be used and expiration time and many other parameters. We can expect the throughput by looking at the delay values and vice versa as the results shows.

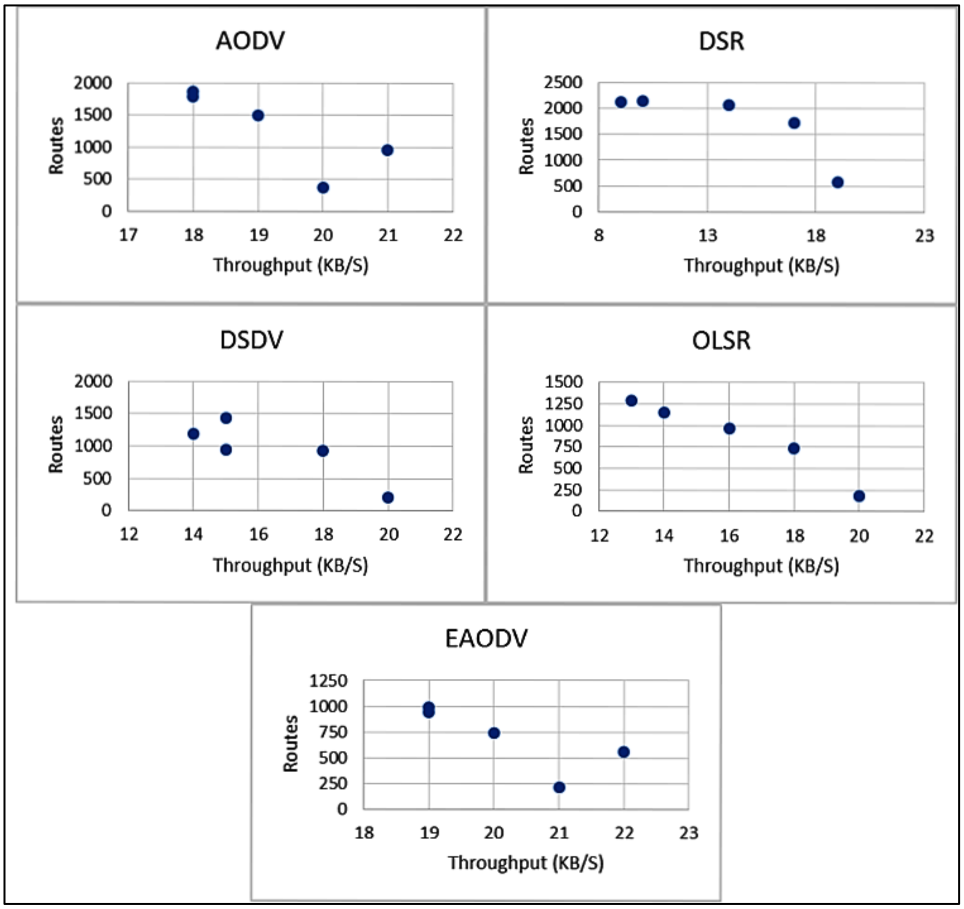


Figure 6. 12: Throughput vs. Number of routes

The number of routes used by the routing protocol to achieve its mission in delivering the required data packets. The number of routes could affect the throughput and results in lowering the total throughput, figure 6.6 shows the relation between the total number of routes used and the average throughput. We notice that the network achieve higher throughput when the number of routes is the minimum. This occurs because the number of routes used is a result of unstable and very changing and dynamic network and hence the total throughput is decreased and lower amounts of data are delivered successfully per unit of time.

6.6 conclusions and future work

The new enhanced model of AODV shows better results in terms of throughput, packet delivery fraction and overhead, and successfully enhanced the network lifetime. This happened because the algorithm successfully balancing:

(1) The Need for distributing the load over larger number of nodes in the network to prolong the network lifetime. This is done by calculating the total energy levels of all nodes in the candidate route and only selecting the routes with higher level of total energy. This way the links with low level of energy will be kept longer and used later on for further routing processes.

(2) And the need to find routes that has higher stability and lasts for longer period of time, this is done by estimating the entire route life time by calculating the speed and direction of movement of each link between any 2 neighbor nodes in that route.

Using only hop count metric is not enough and may lead to degradation in performance because of power loss in specific nodes. The ordinary AODV is highly adaptive to dynamic networks, but still needs more enhancements in terms of power and high dynamic networks.

Our model fails to enhance the delay because it uses routes with larger number of hops and hence the packets needs more time to reach their destinations, but in general the delay still acceptable as it provides a good quality of service for the entire network.

Our future work focuses in enhancing the algorithm in terms of minimizing the delay by optimizing the routes and also minimizing the overhead to the minimum compared to proactive protocols like DSDV.

The other part of our future work plans focuses on the security issues concerning MANET, a major problem in MANET that it is prone to security attacks and the ordinary routing protocols does not provide any mean of security for the network. The security issues needs more work to be done and a central administrative unit to control and monitor the network activities and find the nodes with suspicious behavior and exclude them. Identifying suspicious behavior is easily done and less costly when work is done using special nodes, if all nodes in the network has a policy to monitor the network and identifying any security breaches, this will result in degradation in performance especially in terms of overhead and delay. Hence the security work is better done by specific nodes in the network, we already began this work by proposing a model in clustering the network into logical operational clusters. This model is based on selecting specific nodes to act as administrative units to control their cluster citizens, these nodes are called cluster heads (CH). Those cluster heads are selected based on several metrics like power, degree of connectivity and node internal specifications and local resources, and responsible for monitoring the network and controlling the routing process.

References

[1] Charles E.Perkins, “Ad hoc Networking”, Addison Wesley , 2001.

[2] Subir Kumar Sarkar, T.G. Basavaraju, C. Puttamadappa “Ad Hoc M obile Wireless Networks: Princip les, Protocols and Ap p lications” , Auerbach Publications – Taylor & Francis Group, 2008.

[3] Priy anka Goy al, Vinti Parmar, Rahul Rishi “MANET: Vulnerabilities, Challenges, Attacks, Ap p lication”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893.

[4] Lesiuk, B. Cameron. "Routing in ad hoc networks of mobile hosts." ed. Victoria, BC, Canada http://www. ghost. lesiuk. org/AdoHoc/adhoc (1998).

[5] Feeney, Laura Marie. "A taxonomy for routing protocols in mobile ad hoc networks." SICS Research Report (1999).

[6] S. Giannoulis, C. Antonopoulos, E. Topalis, S. Koubias “ZRP versus DSR and TORA: A comprehensive survey on ZRP performance” 10th IEEE Conference Emerging Technologies and Factory Automation, Greece, 2005.

[7] Tanenbaum Andrew S.: Computer Networks, Prentice Hall, Inc., 1996, ISBN 7-302-02410-3.

[8] Tang, Linpeng, and Qin Liu. "A Survey on Distance Vector Routing Protocols." arXiv preprint arXiv:1111.1514 (2011).

[9] A. Shrestha, and F. Tekiner, “Investigation of MANET routing protocols for mobility and scalability” Int. Conference on Parallel and Distributed Computing, Applications and Technologies, Higashi Hiroshima, 2009.

[10] Lang, Daniel. "On the evaluation and classification of routing protocols for mobile ad hoc networks." München, Techn. Univ., Diss. Dokt (2006).

[11] Kuosmanen, Petteri. "Classification of ad hoc routing protocols." Finnish Defence Forces, Naval Academy, Finland, petteri. kuosmanen@ mil. fi (2002).

[12] Swidan, Andraws, et al. "Mobility and Direction Aware Ad-hoc on Demand Distance Vector Routing Protocol." Procedia Computer Science 94 (2016): 49-56.

[13] Cadger, Fraser, et al. "Location and mobility-aware routing for improving multimedia streaming performance in MANETs." Wireless Personal Communications 86.3 (2016): 1653-1672.

[14] Khalaf, Mustafa Bani, Ahmed Y. Al-Dubai, and Geyong Min. "New efficient velocity-aware probabilistic route discovery schemes for high mobility Ad hoc networks." Journal of Computer and System Sciences 81.1 (2015): 97-109.

[15] Huang, Jincheng, Huihui Xiang, and Yaheng Zhang. "Stable AODV Routing Protocol with Energy-aware in Mobile Ad Hoc Network." JNW 9.9 (2014): 2433-2440.

[16] Cherif, Moussa Ali, Mohamed Kamel Feraoun, and Sofiane Boukli Hacene. "Link quality and MAC-overhead aware predictive preemptive multipath routing protocol for mobile ad hoc networks." International Journal of Communication Networks and Information Security 5.3 (2013): 210.

[17] Chaudhari, Shilpa Shashikant, and Rajashekhar C. Biradar. "Traffic and mobility aware resource prediction using cognitive agent in mobile ad hoc networks." Journal of Network and Computer Applications 72 (2016): 87-103.

[18] Yasin, Adwan, Salah Jabareen, and Iyas Al Suqi. "Enhancing the connectivity of Mobile Ad-hoc Networks by considering the Power, mobility, and activity of nodes." International Journal of Computer Science Issues (IJCSI) 11.2 (2014): 140.

[19] C. E. Perkins, E. M. Belding-Royer, and S. Das. Ad hoc OnDemand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[20] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, Ad hoc Networking, pages 173–219. Addison-Wesley, 2000.

[21] M. S. Corson and A. Ephremides. A Distributed Routing Algorithm for Mobile Wireless Networks. ACM J. Wireless Networks, 1(1), Jan 1995.

[22] C. Perkins and P. Bhagwat. Routing over Multi-hop Wireless Network of Mobile Computers. SIG-COMM '94: Computer Communications Review, (24)4: 234-244, OCT 1994.

[23] Tang, Linpeng, and Qin Liu. "A Survey on Distance Vector Routing Protocols." arXiv preprint arXiv: 1111.1514 (2011).

[24] Xiaoyan Hong, Kaixin Xu and Mario Gerla "Scalable Routing Protocols for Mobile Ad Hoc Networks." Computer Science Department, University of California, Los Angeles, August 2002.

[25] Broch, Josh, et al. "A performance comparison of multi-hop wireless ad hoc network routing protocols." Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking. ACM, 1998.

[26] Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." Ad hoc networking 5 (2001): 139-172.

[27] V. Park and S. Corson, Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification IETF Internet draft (1998).

[28] Park, Vincent D., and M. Scott Corson. "A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing." Computers and Communications, 1998. ISCC'98. Proceedings. Third IEEE Symposium on. IEEE, 1998.

[29] Perkins, Charles E., and Pravin Bhagwat. "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers." ACM SIGCOMM Computer Communication Review. Vol. 24. No. 4. ACM, 1994.

[30] Jacquet, Philippe, et al. "Optimized link state routing protocol for ad hoc networks." Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International. IEEE, 2001.

[31] ETSI STC-RES10 Committee. Radio Equipment and Systems: High Performance Radio Local Area Network (HIPERLAN) Type 1, Functional specifications, June 1996. ETS 300-652.

[32] A. Qayyum, A. Laouiti, L. Viennot, Multipoint relaying technique for flooding broadcast messages in mobile wireless networks, HICSS: Hawai International Conference on System Sciences, January 2002, Hawai, USA.

[33] A. S. Tanenbaum, Computer Networks, Prentice Hall, 1996.

[34] Adjih, Cédric, et al. Experiments with OLSR Routing in a MANET. CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE AT INRIA ROCQUENCOURT (FRANCE), 2006.

[35] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET ondemand (DYMO) routing protocol. Internet-Draft Version 6, IETF, October 2006. draft-ietf-manet-dymo-06.txt, (Work in Progress).

[36] Ian D. Chakeres and Charles E. Perkins. Dynamic MANET ondemand (DYMO) routing protocol. Internet-Draft Version 4, IETF, March 2006. draft-ietf-manet-dymo-04.txt, (Work in Progress).

[37] "Implementing and evaluating the DYMO routing protocol." PhD diss., Aarhus Universitet, Datalogisk Institut, 2007.

[38] S. PalChaudhuri and D. B. Johnson, ―Power Mode Scheduling for Ad Hoc Networks‖, IEEE Int. Conf. on Network Protocols , PP.192-193, Nov 2002

[39] N. Tantubay, D. R. Gautam and M. K. Dhariwal, ― A Review Power Conservation In Wireless Mobile Ad hoc Network (MANET)‖, International Journal of Computer Science Issues, Vol. 8, PP. 1694- 0814, 2011.

[40] Fotino, Marco, et al. "Evaluating energy consumption of proactive and reactive routing protocols in a MANET." *Wireless Sensor and Actor Networks*. Springer US, 2007. 119-130.

[41] Fall, Kevin, and Kannan Varadhan. "The network simulator (ns-2)." *URL: http://www. isi. edu/nsnam/ns* (2007).

[42] Johnson, David B., et al. "The cmu monarch project's wireless and mobility extensions to ns." *Proc. of 42nd Internet Engineering Task Force* (1998).

[43] PalChaudhuri, Santashil, and David B. Johnson. "Power mode scheduling for ad hoc networks." Network Protocols, 2002. Proceedings. 10th IEEE International Conference on. IEEE, 2002.

[44] Liang Qin, Pro-Active Route Maintenance in DSR, Thesis, August 2001.

[45] FanBai, Ahmed Helmy. "A survey of mobility models in wireless Ad Hoc Networks." University of Southern California, USA.

[46] Corson, Scott, and Joseph Macker. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. No. RFC 2501. 1998.

[47] Zhong, Yi Lu Yuhui, and B. BHARGAVA. "Packet Loss in Mobile AdHoc Networks." Bharat Bhargava Purdue University, bb@cs.purdue.edu (2003).

[48] Zhang Jianwu, Zhang Lu "Research on Distance Measurement Based on RSSI of ZigBee" CCCM IEEE 2009.

[49] Neeraj Choudhary, Ajay K Sharma "Performance Evaluation of LR-WPAN for different Path-Loss Models" International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010.

[50] Adwan Yasin, Salah Jabareen, "Adaptive Weighted Clustering Algorithm for Mobile Ad-hoc Networks", International Journal of Computer Network and Information Security (IJCNIS), Vol.8, No.4, pp.30-36, 2016.DOI: 10.5815/ijcnis.2016.04.04.

[51] Gupta, Er Samiti, and Er Naveen Bilandi. "A Comparative Analysis of OLSR, DSR and ZRP Routing Protocols in MANETs." (2014).

[52] Amin, Abu Bony, and Choton Kanti Das. "Prominence of Different Routing Protocols in MANET for Heterogeneous Communication Environment." International Journal of Computer Applications 95.1 (2014).

[53] Nazir, Muhammad Kashif, Rameez U. Rehman, and Atif Nazir. "A Novel Review on Security and Routing Protocols in MANET." Communications and Network 8.04 (2016): 205.

[54] Sharma, Charu, and Jaspreet Kaur. "Literature Survey Of AODV And DSR Reactive Routing Protocols." ICAET, IJCA (2015): 14-17.

الاتصال والدقة في شبكات الاتصال الخاص

شبكات الاتصال الخاص هي عبارة عن نوع من الشبكات التي تربط بين مجموعة من الاجهزة المزودة بمعالجات شبكة لا سلكية, وتختلف هذه الشبكات عن الشبكات الاسلكية التقليدية بانه لا يوجد موجه رئيسي ليقوم بادارة الاجهزة مثل نقاط الوصول. لذلك فان الاجهزة الموجودة في هذه الشبكات تعمل كموجه لتمرير حزم البيانات لغيره من الاجهزة الموجودة في الشبكة. وما يميز هذه الشبكات ايضا هو عدم ثبات البنية, اي ان البنية تتغير باستمرار بسبب حركة الاجهزة المستمرة او بسبب محدودية المصادر فيها مثل محدودية مصدر الطاقة لان هذه الاجهزة لاسلكية وتعمل باستخدام البطاريات وذلك محدودية مصادر المعالجة ومحدودية عرض النطاق الترددي.

بسبب وجود هذه الخصائص المميزة لهذه الشبكات فان الحاجة لوجود بروتوكولات قادرة على التعامل معها تزداد وهذه البروتوكولات يجب ان تكون قادرة على ادارة الشبكة وضمان مستوى عالي من الدقة والاتصال وتوفير جودة وكمية خدمة مناسبة. هناك ايضا العديد من المشاكل التي تترتب على استخدام هذه الشبكات منها مشاكل الحركة الدائمة للاجهزة, ومحدودية مصادر الطاق ومحدودية النطاق الترددي للراوبط بين الاجهزة وكذلك مشاكل الامان في الشبكات, لذلك فان تصميم بروتوكول مناسب ليتعامل مع كل هذه العوامل والمتغيرات يصبح مهمة صعبة وبحاجة الى تطوير خوارزميات جديدة, لان الخوارزميات المستخدمة في الشبكات التقليدية غير قادرة على ادارة مثل هذه الشبكات وتقديم مستوى خدمة مناسب.

في هذه الدراسة قمنا بمحاكاة وتقييم اربعة من البروتوكولات المصممة للتعامل مع شبكات الاتصال الخاص, التقييم شمل مجموعة من مقاييس الاداء مثل الانتاجية والتأخير وكذلك طول حياة الشبكة ونسبة الايصال بالاضافة لعدة معايير اخرى, قمنا بجمع هذه النتائج باستخدام برنامج محاكاة الشبكات الاصدار الثاني, وقمنا بتثبيت عدد من المتغيرات وتغيير متغيرات اخرى. النتائج التي حصلنا عليها تشير الى تفاوت حاد في اداء البروتوكولات وخصوصا في الظروف الحادة مثل سرعة حركة العملاء داخل الشبكة وكذلك محدودية مصادر الطاقة لها.

في القسم الاخير من الدراسة قمنا باضافة بعض التحسينات على خوارزمية عمل احد هذه البروتوكولات لتمكين البروتوكول من تخفيض عدد رسائل التحكم اللازمة وكذلك تمديد طول مدة حياة الشبكة لوقت اطول بالاضفة الى ان النتائج اظهرت تحسنا في اداء البروتوكول من حيث الانتاجية وكمية البيانات المسلمة. هذه الخورازمية تعتمد بالاساس على اختيار المسارات الاكثر ثباتا والاعلى طاقة لتمرير حزم البيانات من خلالها.