Democratic and Popular Republic of Algeria Ministry of Higher Education and Scientific Research

Faculty of Exact Sciences and Sciences of Nature and Life

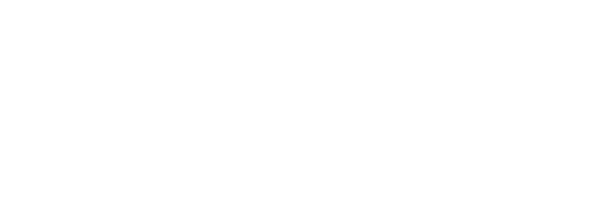
Tebessa University

Department of Maths and Computing Science

## Master’s Thesis

In

Networks and Security Theme



|  |  |  |
| --- | --- | --- |
| **Presented by :** |  | |
| **Rezzoug Sarra** |
| **Messaadi Mehdi** |
| **President :** Dr.Derdour | **Jury Members:**  M.A.A | Tebessa University |
| **supervisor :** M. Mahmoudi | M.A.A | Tebessa University |
| **Examiner :** A.Azzeddine | M.A.A | Tebessa University |

## 2016/2017

**Acknowledgement**

We thank Allah the almighty first and foremost, for having bestowed upon us the strength and determination to complete this project.

We would like to thank our advisor, Mr. Mahmoudi Rachid, who has given us plenty of helpful advices, guidance, and support in each step from the beginning to the completion of our project.

We also want to thank the esteemed members of the jury for giving us the honor and pleasure of reviewing and evaluating our work.

Finally, we express our most sincere gratitude to our parents, professors, colleagues, friends, and all of those who have accompanied us throughout our curriculum and given us the strength and the courage to succeed.

A mobile Ad Hoc network, is a set of mobile nodes that move freely within a certain geographical area without any pre-existing fixed infrastructure.

Routing is the most important problem in ad hoc networks, because of mobility of nodes it is very difficult to locate a destination at a given moment.

Several routing protocols for ad hoc networks have been proposed, these protocols try to maximize performance of the network. Many research tested AODV protocol and proved that is the most performing out of the MANET protocols.

Our project aims to study the impact of mobility on the reliability of AODV protocol and propose a new modified AODV with speed metric to select the best route. The main goal of this approach is to improve the reliability of AODV.

The results show that high node speed has a negative influence, and our modified AODV provides better results than the default AODV.

**Key words:** MANET, mobility, reliability, AODV.

Un réseau ad hoc mobile, est un ensemble de nœuds mobiles qui se déplacent librement dans une certaine zone géographique sans aucune infrastructure fixe préexistante.

Le routage est le problème le plus important dans les réseaux ad hoc, en raison de la mobilité

des nœuds, il est très difficile de localiser une destination à un moment donné.

Plusieurs protocoles de routage pour les réseaux ad hoc ont été proposés, ces protocoles tentent de maximiser les performances du réseau. Plusieurs recherches ont testé le protocole AODV et ont prouvé qu'il est le plus performant parmi les protocoles MANET.

Notre projet vise à étudier l'impact de la mobilité sur la fiabilité du protocole AODV et à proposer un nouveau AODV modifié avec une métrique de vitesse pour sélectionner le meilleur chemin. L'objectif principal de cette approche est d'améliorer la fiabilité d'AODV. Les résultats montrent que la vitesse élevée des nœuds a une influence négative, et notre AODV modifié fournit de meilleurs résultats que l'AODV par défaut.

**Mots clés:** Manet, mobilité, fiabilité, AODV.

# الملخص

شبكة Hoc Ad هي عبارة عن مجموعة من العقد التي تتحرك بحرية داخل منطقة جغرافية معينة دون أي بنية تحتية ثابتة

موجودة مسبقا. التوجيه هو أهم مشكلة في شبكات Hoc Ad، وذلك بسبب ديناميكية العقد، فإنه من الصعب جدا تحديد موقع واتجاه حركة

العقد في مرحلة ما. وقد اقترحت عدة بروتوكوالت توجيه لشبكات Hoc Ad ،بهدف تحسين أداء الشبكة .لقد اختبرت دراسات عديدة

بروتوكول AODV وأثبت أنه األكثر كفاءة بين بروتوكوالت .MANET

ويهدف مشروعنا لدراسة تأثير التنقل على فعالية بروتوكول AODV واقتراح AODV جديد و مغير مع مقياس السرعة

لتحديد أفضل طريق. والهدف الرئيسي من هذا النهج هو تحسين فعالية .AODV أظهرت النتائج أن سرعة عالية من العقد له تأثير سلبي, وان AODV المعدل لدينا يوفر نتائج احسن من ال

. االصليAODV

الكلمات المفتاحية : شبكة MANET , شبكة ديناميكية , فعالية بروتوكول الشبكة .

**List of figures:**

# Chapter I:

**Figure I.1:** Mobile networks with infrastructure 4

**Figure I.2:** Mobile ad hoc network. 5

**Figure I.3:** Changing the topology of an ad hoc network. 5

**Figure I.4:** Classification of ad hoc routing protocols 10

**Figure I.5:** Neighbor detection using HELLO messages 11

**Figure I.6:** Ad hoc network topology 13

**Figure I.7:** A cluster network organization 15

**Figure I.8:** Building record route during route discovery 16

**Figure I.9:** Propagation of route reply with route record. 16

**Figure I.10:** Dividing the network into zones by ZHLS protocol 18

**Figure I.11:** Zone routing protocol 19

# Chapter II:

**Figure II.1:** Routing table format 24

**Figure II.2:** RREQ packet format 24

**Figure II.3:** Route reply packet 25

**Figure II.4:** Route error packet 26

**Figure II.5:** Propagation of RREQ 27

**Figure II.6:** Propagation of RREP 28

**Figure II.7:** Initiating route discovery 29

**Figure II.8:** Broadcast RREQ to C 30

**Figure II.9:** Broadcast RREQ to D 30

**Figure II.10:** Broadcast RREQ to E 31

**Figure II.11:** Destination node E creates a RREP 31

**Figure II.12:** Destination node E unicasts RREP to D 32

**Figure II.13:** Node D unicasts RREP to C 32

**Figure II.14:** Node C unicasts RREP to source node A 33

**Figure II.15:** Route maintenance 34

**Chapter III:**

|  |  |  |
| --- | --- | --- |
| **Figure** | **III.1:** | Network simulators 42 |
| **Figure** | **III.2:** | Project editor interfaces 44 |
| **Figure** | **III.3:** | Project editor icons 44 |
| **Figure** | **III.4:** | Node editor interface 45 |
| **Figure** | **III.5:** | Process editor interface 46 |
| **Figure** | **III.6:** | ICI editor interface 46 |
| **Figure** | **III.7:** | Packet format editor interface 47 |
| **Figure** | **III.8:** | Choose individual statistics 47 |
| **Figure** | **III.9:** | Configuring run simulation 48 |
| **Figure** | **III.10:** | View results 48 |

**Chapter IV:**

**Figure IV.1:** Proposition route discovery 59

**Figure IV.2:** RREQ of default AODV 60

**Figure IV.3:** RREQ of modified AODV 60

**Figure IV.4:** Opnet modeler 14.5 61

**Figure IV.5:** Simulation network 62

**Figure IV.6:** AODV configuration 62

**Chapter V:**

|  |  |  |
| --- | --- | --- |
| **Figure** | **V.1:** | total packets dropped for 20 nodes 65 |
| **Figure** | **V.2:** | total packets dropped for 25 nodes 65 |
| **Figure** | **V.3:** | delay for 20 nodes 66 |
| **Figure** | **V.4:** | delay for 25 nodes 66 |
| **Figure** | **V.5:** | throughput for 20 nodes 67 |
| **Figure** | **V.6:** | throughput for 25 nodes 67 |
| **Figure** | **V.7:** | total packets dropped versus number of nodes 68 |
| **Figure** | **V.8:** | End to End Delay versus number of nodes 69 |
| **Figure** | **V.9:** | Throughput versus number of nodes 69 |
| **Figure** | **V.10:** | Total packets dropped with different speed 70 |
| **Figure** | **V.11:** | End to End delay with different speed 71 |
| **Figure** | **V.12:** | Throughput with different speed 71 |
| **Figure** | **V.13:** | Total packets dropped under different mobility models 72 |
| **Figure** | **V.14:** | End to end delay under different mobility models 73 |
| **Figure** | **V.15:** | Throughput under different mobility models 73 |
| **Figure** | **V.16:** | Total packets dropped comparison 74 |
| **Figure** | **V.17:** | delay comparison 75 |
| **Figure** | **V.18:** | Throughput comparison 75 |

**Figure V.19:** total packets dropped comparison between default and modified AODV..76

**Figure V.20:** delay comparison between default and modified AODV 77

**Figure V.21:** Throughput comparison between default and modified AODV 77

**Figure V.22:** total packets dropped comparison between default and modified AODV 78

**Figure V.23:** delay comparison between default and modified AODV 79

**Figure V.24:** Throughput comparison between default and modified AODV 79

**List of Tables:**

# Chapter I:

**Table I.1:** 13

# Chapter V:

**Table V.1:** Network Parameters 64

**Table V.2:** Simulation scenarios 64

**Table V.3:** Simulation scenarios 70

**Table V.4:** Simulation scenarios under mobility models 72

**Table V.5:** First Test 76

**Table V.6:** Second Test 78

# Table of contents:

[General introduction: 1](#_TOC_250004)

Chapter I: Ad hoc networks: 4

* 1. Introduction: 4
  2. Mobile Networks 4

1.2.1. Mobile networks with infrastructure: 4

1.2.2 Mobile Ad Hoc Networks 5

* + - 1. Characteristics of Ad Hoc networks: 5
      2. Applications of Ad Hoc networks: 6
      3. Advantages: 7
      4. Disadvantages: 8
  1. Routing in mobile ad hoc network: 8
     1. The difficulty of routing in Ad hoc networks: 8
     2. Routing constraints in ad hoc networks: 9
  2. Classification of Ad hoc routing protocols: 9
     1. Proactive routing protocols: 10
        1. Optimized Link State Routing Protocol (OLSR): ………10
        2. Dynamic Destination-Sequenced Distance- Vector 12
        3. Advantages of proactive protocols: 14
        4. Disadvantages of proactive protocols: 14
     2. Reactive routing protocols: 14
        1. Cluster-based Routing Protocol (CBRP): 14
        2. Dynamic Source Routing (DSR): 15
        3. Advantages of reactive protocols: 16
        4. Disadvantages of reactive protocols: 17
     3. Hybrid routing protocols: 17
        1. Zone Routing Protocol (ZRP): 17
        2. Zone Based Hierarchical Link State Routing Protocol…..18
  3. Security in mobile ad hoc network: 19
     1. Possible Attacks in Routing Protocols: 20
        1. Deleting packet attacks: 20
        2. Attacks by Changing Routing Information: 20
        3. Spoofing Attack: 20
  4. [Conclusion: 21](#_TOC_250003)

Chapter II: AODV routing protocol: 22

* 1. Introduction: 22
  2. Definition of AODV 22
  3. Characteristics: 22
  4. Terminology of AODV 23
  5. Routing Table: 24
  6. Messages Format: 24
     1. Route Request (RREQ): 24
     2. Route Reply (RREP): 25
     3. Route Error (RERR): 26
  7. Functioning: 27
     1. Route discovery: 27
        1. Illustration of route establishment in AODV: 29
     2. Route maintenance: 33
        1. Illustration of route maintenance in AODV: 33
  8. Advantages of AODV 34
  9. Disadvantages of AODV: 34
  10. Security vulnerabilities of AODV 35

II.11: Conclusion: 35

Chapter III: Simulation: 36

* 1. [Introduction: 36](#_TOC_250002)
  2. Definition of simulation: 36
     1. Cases of simulation: 36
     2. Types of simulations: 37
     3. Advantages and disadvantages of simulations: 37
  3. Modeling: 38
     1. Definition: 38
     2. Types of models: 39
     3. Calibration, verification, and validation of models: 40
     4. Applications of simulation models: 40
  4. Definition of network simulation: 40
  5. Network Simulators: 41
  6. Opnet Modeler: 42
     1. Definition: 42
     2. Opnet characteristics and features: 42
     3. Opnet Applications: 43
     4. Opnet editors: 44
     5. Running a Simulation: 47
        1. Statistic Collection: 47
        2. Configuring Simulations: 48
        3. View results: 48

[III.7 Conclusion: 49](#_TOC_250001)

Chapter IV: Impact of mobility on reliability of AODV: 50

* 1. introduction: 50
  2. Mobility in ad hoc networks: 50
     1. definition: 50
     2. mobility models: 51
  3. Related works 51
  4. Impact of mobility on reliability of AODV 57
     1. presentation: 57
     2. different tests or investigations: 57
     3. modifying AODV parameters: 58
  5. AODV with new speed metric: 58
     1. source code modification: 60
     2. parameters used in the network: 60
  6. Implementation of our contribution: 61
     1. Chosen simulator: 61
     2. network simulation: 61
  7. [Conclusion: 63](#_TOC_250000)

Chapter V: Simulation and Results 64

* 1. Introduction: 64
  2. Simulation Setup: 64
  3. investigation of speed: 64
     1. total packets dropped: 65
     2. End to End delay: 66
     3. Throughput: 67
     4. conclusion of investigation of speed: 68
  4. investigation of density: 68
     1. total packets dropped: 68
     2. End to End delay: 69
     3. Throughput: 69
     4. conclusion of investigation of density: 70
  5. investigation of maximum speed: 70
     1. total packets dropped: 70
     2. End to End delay: 71
     3. Throughput: 71
     4. conclusion of maximum speed: 72
  6. investigation of mobility models: 72
     1. total packets dropped: 72
     2. End to End delay: 73
     3. Throughput: 73
     4. Conclusion of mobility models: 74
  7. Modifying AODV parameter: 74
     1. total packets dropped: 74
     2. End to End delay: 74
     3. Throughput: 75
     4. Conclusion: 75
  8. AODV with new speed metric: 76
     1. First Test: 76
        1. Total packets dropped: 76
        2. end to end delay: 77
        3. Throughput: 77
     2. Second Test: 78
        1. Total packets dropped: 78
        2. End to End delay: 79
        3. Throughput: 79
     3. conclusion of the two tests: 80

V.9 conclusion: 80

## General conclusion: 81

**References** 82

# General Introduction:

In recent years, the world is experiencing a great evolution of many standards of connectivity and wireless technologies. These technologies allow the emergence of a new type of network, Mobile Ad Hoc Network, or MANET. These can offer the possibility of quick and impromptu (Ad Hoc) connections and also offer the possibility of automatic connections between the mobile devices. Mobile ad hoc networks (MANETs) are widely used in wireless networks consisting of mobile devices that communicate in the absence of any centralized support.

Ad hoc networks are self-organized and nodes that make up a network can multiples types of roles, which makes MANETs economic and easily installed.

There are many applications for Ad hoc networks. They are used in vehicular communications where they allow for the development of artificial intelligences that aid in the linking and information exchange between vehicles in cases of roadblocks, accidents, emergencies…etc. Another important application is in military. Armies have always been in the need for communications that are not fixed in a single location, but instead can still be optimal while military units embark on deployment and fast operations. MANETs in this case can be configured in many ways to aid military missions. MANETs can also be used in emergencies that occur in cases of natural disasters and catastrophes (earthquakes, floods, tornadoes…etc.) with their infrastructure-less nature, by allowing a continuous communication between the numerous groups of rescue teams as they move, often in a fast pace, between many different locations of the disaster-struck area.

Routing in Ad hoc networks is an important factor, since every node (mobile entity) can act as a router, transmit data packets, and actively achieve communication with other nodes. For this reason, routing protocols have a high significance in MANETs. Three categories of routing protocols can be distinguished in Ad hoc networks. Proactive, reactive, and hybrid. Each protocol in the aforementioned categories manages routing information using its own approach. In that context, we have chosen to concentrate our work on the AODV (Ad hoc on demand distance vector) protocol.

AODV is a distance vector protocol capable of both unicast and multicast routing. It was one of the first routing protocols created for Ad hoc network, which allowed it to evolve and gain a firmer place among MANET protocols throughout the years. Due to the protocol’s maturity, simplicity, and other advantages, many works that have done comparative research between AODV and other MANET protocols found that AODV generally outperforms the rest, whether it’s in a network with a high number of nodes, or a large network, or vice versa…

However, despite AODV’s advantages, Ad hoc networks have problems that can affect the reliability and performance of routing protocols, and also of the network itself. Between security issues, bandwidth limitations, packet losses due to transmission errors, Ad hoc networks have many challenges that require addressing. One of the more important issues MANETs are facing is mobility. Since the very nature of nodes in MANETs is mobile and unfixed, AODV’s reliability can be affected in the network as a result.

# The problematic:

Mobility is an important characteristic in MANET. Our problematic is to study it’s influence on reliability of AODV and propose a new metric for AODV to select the best route in purpose to enhance its reliability.

We can reformulate our problematic by the following sub problems:

 What are the tools of implementation and the method used for this evaluation.  Prove the impact of mobility on the reliability.

 How to change number of hops metric by speed metric to select best route.  How to evaluate the network performance by our modification.

 What are the evaluation parameters of network reliability.

# Our objectives:

 Create a MANET network, routed with AODV, using simulations with OPNET 14.5

 Study the impact of mobility on reliability of AODV based on node’s speed, mobility models, and the impact of speed in a large network.

 Modifying the AODV source code, by changing the metric of selection of best route from number of hops to speed.

 Using graphs results to compare between our modified AODV and the default AODV, based on reliability parameters.

 Comparison of simulation results of default and Optimized AODV protocol in regards to Throughput, delay, and number of packets dropped.

## This master thesis is organized as shown below:

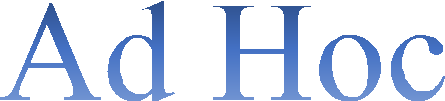
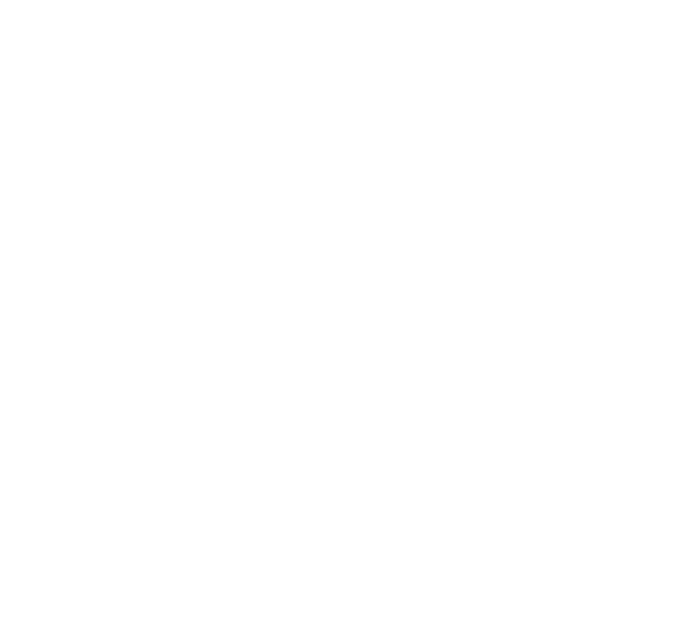
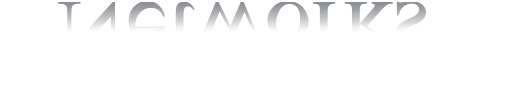
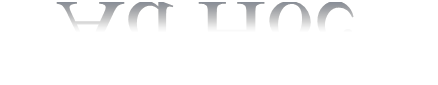
**In the first chapter,** we have introduced ad hoc networks while highlighting their characteristics and properties. We have also defined the routing problem, which is crucial in MANETs.

**In the second chapter,** we presented the AODV protocol by clarifying how it works, the types of packets it deals with, and how it manages and establishes routes.

**The third chapter,** contains explanations detailing simulations, modeling, and our chosen simulation platform OPNET, with precise presentation of its main features and functions.

**The forth chapter,** comprises our different investigations of mobility and our modification of AODV with a new speed metric.

**In the fifth chapter,** we showed the simulation results of our study, and the results of the comparison between the default and modified AODV.



# Introduction:

Recent technological developments in the field of wireless communication and the emergence of portable computing units are now pushing researchers to make efforts to achieve the goal of networks: "Access to information anytime, from anywhere ".

The concept of mobile ad hoc networks tries to extend the notions of mobility to all the components of the environment. Here, unlike networks based on infrastructure communication (cellular), no centralized administration is available, it is the mobile hosts themselves that form a network infrastructure. No assumption or limitation is made on the size of the ad hoc network, as it may contain hundreds or thousands of mobile units.

In this chapter, we will introduce mobile ad hoc networks, their features, applications, and the most important aspect in this type of network, the routing problem.

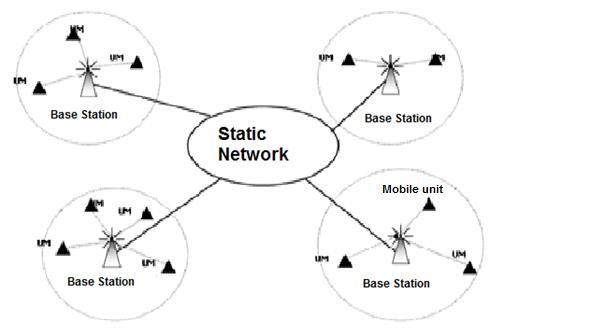
# Mobile Networks

A mobile environment is a system of mobile sites that allows users to access information regardless of their geographic location. Mobile or wireless networks can be categorized into infrastructure-based and Ad Hoc networks (infrastructure-less).[1]

## Mobile networks with infrastructure

In infrastructure mode, also known as the Basic Service Set (BSS) mode, some fixed sites called Mobile Support Station (MS) or Base Station (SB), are equipped with a wireless communication interface for direct communication with Mobile sites or units (MUs), located in a limited geographical area, called a cell.

Each base station corresponds to a cell from which mobile units can transmit and receive messages. While the fixed sites are interconnected with each other through a wired, generally reliable and fast communication network, wireless links have a limited bandwidth that severely reduces the volume of information exchanged. In this model, a mobile unit can only be directly-connected, at a given instant, to a single base station.[2]



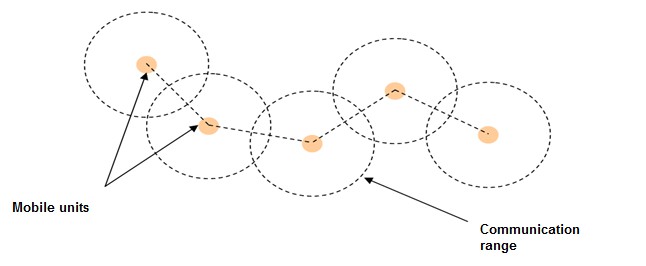
## Figure I.1 Mobile networks with infrastructure [1]

* + 1. **Mobile Ad Hoc Networks**

A mobile Ad Hoc network, generally called MANET , is a set of mobile nodes that move freely within a certain geographical area without any pre-existing fixed infrastructure. A node in the ad hoc network communicates with another node directly (using its wireless interface) if it is within its transmission range. If it isnt, the communication is done indirectly via other

nodes of the network . Each node in the ad hoc network must behave as a terminal, and also as a router, and participate in the discovery and maintenance of the paths between the nodes of the network.

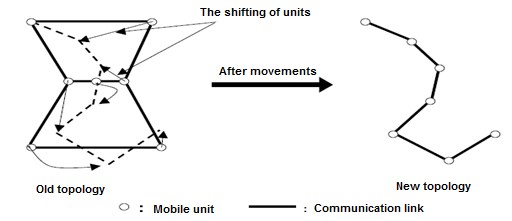
There is no size limitation in an ad hoc network. It can contain tens or thousands of nodes.[3]



## Figure I.2 mobile ad hoc network [1]

* + - 1. **Characteristics of Ad Hoc networks**
         * **dynamic topology:** The mobile units of the network move freely and arbitrarily.

Therefore, the topology of the network can change at unpredictable times, and in a fast

and

random way.

## Figure I.3: Changing the topology of an ad hoc network [2]

* + - * + **Limited bandwidth:** One of the primary characteristics of networks based on wireless communication is the use of a shared communication medium. This sharing means that the bandwidth reserved for a host is modest and limited.
        + **Energy constraints:** Mobile hosts are powered by stand-alone energy sources such as batteries or other consumable sources. The energy parameter must be taken into account in any control performed by the system.
        + **Limited physical security:** Ad hoc mobile networks are more affected by the security parameter than traditional wireline networks. This is justified by the physical constraints and limitations that minimize the control of the transferred data.
        + **Lack of infrastructure:** Ad hoc networks are distinguished from other mobile networks by the lack of pre-existing infrastructure and any kind of centralized administration. Mobile hosts are responsible for establishing and maintaining network connectivity on an ongoing basis.[2]

## Applications of Ad Hoc networks

Ad Hoc networks are used in all applications where deployment of centralized architecture is impossible. Their robustness, low cost and rapid deployment give them access to a wide range of applications, including:

1. Strategic networks:
   * Military communication and movements
   * Automated combat zones b- Emergency services :
   * Operations of search and rescue
   * Disaster salvage
   * Replacing stable infrastructure when environmental disasters occur
   * Police work and fire fighting
   * Assissting doctors and nurses inside hospitals c- Commercial and civilian environment:
     + Electronic-commerce: the abilty to pay electronically, anywhere and anytime
     + Business side: a dynamic access to databses, traveling offices
     + Vehicular services: road or accident help, diffusion of road and weather conditions, taxi cab network, inter-vehicular networks…etc
     + Sport stadiums, trade fairs and shopping malls
     + Networks of visitors established at airports d- Home and enterprise networking :
     + Home/office wireless networking
     + Meeting rooms and conferences
     + Construction sites’ networks
2. Education
   * Layouts of universities and campuses
   * Virtual classrooms
   * Ad hoc communications set during meetings or lectures f- Sensor networks
   * Home appliances: smart sensors embedded in electronics…etc
   * (BAN) Body area networks
   * Data tracking of environmental conditions, animal movements, chemical/biological detection

In general, ad hoc networks are used in any application where the deployment of a wired network infrastructure is too constraining, either because it is difficult to set up or because the duration of the network installation does not justify permanent wiring.[6]

## Advantages :

* **Wireless:** One feature of Ad Hoc networks is the lack of wiring, eliminating all wired connections that are replaced by radio connections.
* **Easy deployment:** The lack of cabling gives you more flexibility and allows you to deploy an Ad Hoc network easily and quickly. This facility can be justified by the lack of a pre- existing infrastructure, thus saving the entire deployment time and Installation of the necessary equipment.
* **Cost:** Deploying an Ad Hoc network does not require the installation of base stations. Mobile nodes are the only physical entities required to deploy.[4]

## Disadvantages:

* **Non-predictable topology:** The constant activity and frequent movement of the nodes of an Ad Hoc network makes its study very difficult. The reason is the rapid change of its topology because of the movement of the nodes.
* **Limited capacities:** In an Ad Hoc network, the configuration of the communication range of the nodes is important. In fact, it must be sufficient to ensure the connectivity of the network. But when the range of the mobiles is increased, the communications require more of energy.
* **Significant error rate:** The risk of collision increases with the number of nodes sharing the same medium therefore the range increases also the risk of collision increses.
* **Security:** Another dilemma of the Ad Hoc networks, which attracts the curiosity of researchers and specialists in this field, is the notion of security. An Ad Hoc network as defined above does not guarantee the confidentiality of information exchange between The nodes unlike in wired network.[7]

# Routing in mobile ad hoc network:

Routing is a method of transmitting information to the right destination through a given network, it consists of ensuring a strategy that guarantees, at any time, the establishment of paths that are correct and efficient between any pair of nodes belonging to the network, which ensures the exchange of messages in a constant manner. Given the limitations of ad hoc networks, path creation must be done with minimal control and bandwidth consumption.

Because of node mobility in ad hoc network it is difficult to locate a destination node at a given time, a routing protocol for ad hoc networks must build and maintain the routes between the different nodes and adapt to the changing topology .

## The difficulty of routing in Ad hoc networks:

An ad hoc network is a set of mobile nodes that are dynamically and arbitrarily scattered in a way where interconnection between nodes can change at any time. A destination host may be out of the communication range of a source host, requiring internal routing by the intermediate nodes to guide the message packets to the correct destination.

The problem that arises in the context of ad hoc networks is the adaptation of the routing method used with the large number of units existing in an environment characterized by modest computing and backup capabilities.[5]

Moreover, practically speaking, it is impossible for a host to be able to keep the routing information concerning all the other nodes, in the case of a voluminous network.

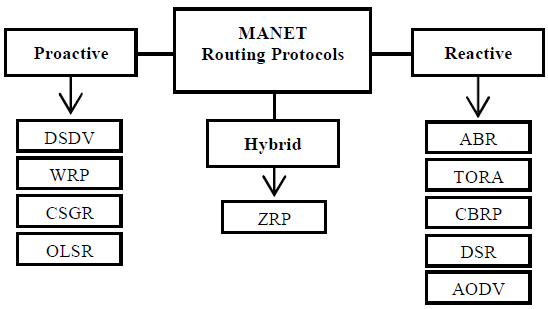
## Routing constraints in ad hoc networks:

The study and the implementation of routing algorithms to ensure the connection of ad hoc networks in the classic sense of the term (any vertex can reach any other), is a complex problem. The environment is dynamic and evolves over time, the topology of the network can change frequently. Therefore, it is important that any routing protocol design should address the following issues:[2]

* **Network Load Minimization**: Network resource optimization has two other sub problems. Avoiding routing loops, and preventing the concentration of traffic around certain nodes or links.
* **Provide support for reliable multi-point communications:** The fact that the paths used to route data packets can evolve should not have an issue with the proper routing of data. The elimination of a link due to breakdown or mobility should ideally increase latency times as little as possible.
* **Ensure optimal routing:** The routing strategy must create optimal paths and be able to take into account different cost metrics (bandwidth, number of links, network resources, etc.). If the creation of optimal paths is a hard problem, the maintenance of such paths can become even more complex, the routing strategy must ensure efficient maintenance of roads with the least possible cost.
* **Latency:** The quality of latency times and paths must increase with every growth in the connectivity of the network.

# Classification of Ad hoc routing protocols

Depending on how to create and maintain routes when routing data, routing protocols can be divided into three categories, proactive protocols, reactive protocols and hybrid protocol. Pro- active protocols establish routes in advance based on periodic exchange of routing tables, while reactive protocols look for routes on demand and hybrid protocol combine the two other categories.[13]



## I.4 classification of ad hoc routing protocol [10]

* + 1. **Proactive routing protocols**

This type uses regular exchange of control messages to maintain routing tables at each node for any destination reachable from it. These tables are maintained, and the routes are saved even if they are not used. The permanent backup of the routing paths is ensured by a continuous exchange of the path update messages.

This approach makes it possible to have a route to each destination immediately when a packet is to be sent.[8]

## Optimized Link State Routing Protocol (OLSR):

The optimized link state routing protocol (OLSR) [11] is an optimization of the link state algorithm, which is the basis for link state routing protocols. The central technique used in this protocol is the utilization of MPRs (Multipoint Relays). In it, every node chooses in its vicinity a group of MPR nodes. This group is chosen in such a way that it covers all nodes that are two hops away. This technique considerably reduces network overload.

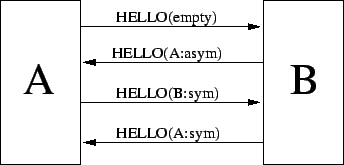
OLSR routing protocol was designed to calculate and recalculate routes, and deliver the optimal routes with the minimum number of hops. For that reason, this process needs the knowledge of the following elements:

* + - * + List of neighboring nodes: The neighboring one hop, or two hop relations. The latter being defined by the exchange of HELLO messages.
        + Link types: Either it is a symmetrical link (Where communication is possible in both directions), or an asymmetrical link (where communication is only possible in one way), or a lost link (when links are lost or non-specified).
        + Network topology: Using Topology Control (TC) messages, OLSR routing protocol uses a topological network table.

## Neighbor discovery:

Every node in the network releases “HELLO” messages sporadically in order to detect its direct neighbors. These “HELLO” messages contain the list of known node neighbors, and their link states. As mentioned above, the link states can either be symmetrical, asymmetrical, lost, or multipoint relay. This last type of link means that it is symmetrical, and that the expeditor of the “HELLO” message has chosen this node as an MPR. “HELLO” messages are released in a set time interval of 2 seconds (default value). These messages are also received by neighboring nodes of one hop, but are not transmitted. This way, “HELLO” messages

allow the discovery of one hop neighboring nodes, and two hop ones for every node. There is an interval that decides the validity of information associated with one hop or two hop neighboring nodes. This interval is defined as 3 \* HELLO\_Interval (Default value).



## Figure I.5: Neighbor detection using HELLO messages.[12]

Based on the exchange of HELLO messages, every node constructs its own database called Link\_Tuple. In it, there is a description of the one hop neighboring of a node, the type of link, the two hop neighboring and the node’s list of MPR.

Using this information, MPRs are selected for every node using one hope neighbors. They are chosen in such a way that they can cover all two hope neighbors. MPR groups are

recalculated every time a change occurs in both one hope, and two hope neighboring.

## Topology discovery:

Every node in the network uses TC messages to maintain network topology information. MPR nodes release a TC message every TC interval, defined by 5 seconds (default value). When an MPR group is altered, the next TC message can be released earlier. All network nodes use flooding to release TC messages, and MPRs reduce the transmission number. Thus, a node could be reached directly, or by its MPR intermediate.[11]

Information regarding neighbor discovery and topology discovery are frequently updated. This data helps nodes calculates routes towards all known destinations. The paths are optimal in regards to hop count since they are calculated using the Dijkstra algorithm.

## Dynamic Destination-Sequenced Distance- Vector (DSDV):

DSDV was designed specifically for mobile networks and is based on the classic idea of Bellman-Ford's distributed algorithm, adding some improvements. Each mobile station maintains a table routing file that contains

* All possible destinations.
* The number of nodes (or jumps) required to reach the destination.
* The sequence number (SN: sequence number) that corresponds to a destination node.

For each node i, the sequence number of destination is associated at each distance entry Dijk, for each neighbor K. the sequence number is used to distinguish between the old and new route, to avoid counting to infinity problem.

In order to maintain the consistency of the routing tables in a rapidly changing topology, each node of the network periodically transmits its routing table to its direct neighbors. The node can also transmit its routing table if the content of the routing table undergoes significant changes in relation to the last content sent. The update therefore depends on two parameters: the time that is the transmission period, and the events (node occurrence, detection of a new neighbor, etc.). The update must allow a mobile unit to locate, in most cases, another unit of the network.[2]

Updating the routing table can be done in two ways:

* A complete update.
* An incremental update.

In the full update, the station transmits the entire routing table to the neighbors, which

requires sending several packets of data. On the other hand, in an incremental update, only the entries that have undergone a change from the last update are sent, which reduces the number of packets transmitted. The way to update the routing tables is linked to the stability of the network. In the case where the network is relatively stable, the incremental update is used to reduce communication traffic. In the opposite case, the number of incremental packets sent increases, so that the complete update is frequent.[2]

An update package contains:

1 - The new incremented sequence number of the sender node. And for each new route: 2 - The address of the destination.

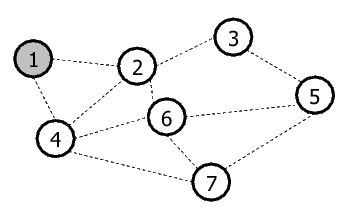
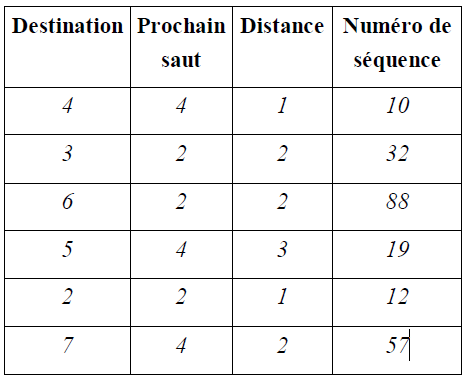
1. - The number of nodes (or jumps) separating the node from the destination.
2. - The sequence number (of the data received from the destination) as stamped by the destination.

The routing data received by a mobile unit is compared with the data already available. The route labeled with the highest value of the sequence number (i.e. the most recent route) is the route used. If two routes have the same sequence number, then the route with the best metric is the one that will be used. The metric used in the calculation of the shortest paths is simply the number of nodes in the path. The values of the metrics of the routes, chosen after reception of the routing data, are incremented.

Changes made to local routing data are immediate ly broadcast to the current set of neighbors. The routes received by a broadcast will also be sent when the receiver sends its routing packets. The receiver must increment the metrics of the routes received before sending, because the receiver represents an additional node that participates in the routing of the messages to the destination.

A broken link is materialized by an infinite value of its metric, i.e. a value greater than the maximum value allowed by the metric. The DSDV eliminates the two problems of routing loop, and that of counting to infinity. However, in this protocol, a mobile unit must wait until it receives the next update initiated by the destination, in order to update the entry associated with that destination in the distance table. This makes the DSDV slow.

Figure (I.5) illustrates the topology of an ad hoc network at a given time and the

Routing corresponding to the node (1) in the DSDV protocol.[12]

## Figure I.6 ad hoc network topology[12] Table I.1 routing table of node 1[12]

* + - 1. **Advantages of proactive protocols**
* Paths are available immediately
* Time saving when requesting a route

## II.4.1.4 Disadvantages of proactive protocols

* Path changes may be more frequent than the request for the path, and the traffic induced by monitoring routing tables and updating messages may be large and partially unnecessary, which wastes the capacity of the wireless network.
* The size of the routing tables grows in accordance to the number of nodes.

## Reactive routing protocols

The reactive routing protocols (also known as on-demand routing protocols) represent the most recent protocols proposed in order to provide routing service in wireless networks.

Routing protocols belonging to this category create and maintain paths as required. When the network needs a path, an overall path discovery procedure is initiated, in order to obtain information.[2]

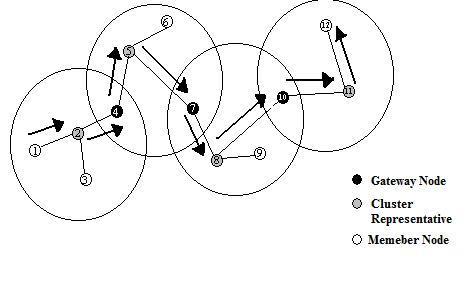
## Cluster-based Routing Protocol (CBRP):

The cluster-based routing protocol (CBRP) divides the network nodes into groups, or clusters. a- **CBRP clusters:**

A given node N that does not have a status (meaning, not a member or a representative of a cluster) activates a timer and releases a HELLO message. When a cluster representative receives this HELLO message, it instantly sends back a reply to the sender. Upon receiving this reply, the given node N changes its state from “Undecided” to “Member”. If this given node N spends a certain amount of time (timeout) waiting for the reply and it has in its possession a bidirectional link toward at least one neighboring node, this node N considers itself a representative of a cluster. In the opposing case, N remains in the “Undecided” state and it repeats the same process. Due to the fast changing nature of topologies of ad hoc networks, undecided nodes have a very short waiting time period.

To be able to conserve the node division in each cluster, every node maintains a neighbors table. Each entry value in this table is associated to a specific neighboring node, and it indicates the link state (unidirectional or bidirectional) and the neighbor’s state (member of the cluster or representative of the cluster). A cluster representative keeps data about members that are a part of its cluster.[2]

The cluster representative has a close cluster table as well. Each data entry in this table is related to a neighboring cluster. An entry contains a cluster identifier (ID) and an identifier to the gateway node with which the cluster could be reached.



## Figure I.7: A cluster network organization[2]

**b- CBRP routing:**

When a source node in CBRP intends to send data to a destination node, it uses flooding to release a route request only to neighboring cluster representatives. A cluster representative that receives a route request uses its cluster members’ table to verify and validate the existence of the destination node in its cluster. If it does exist, the representative immediately sends it the route request. Otherwise, the route request is transferred to the neighboring cluster representatives.

The address of cluster representative is included in the route request, and a representative always ignores each route request it already treated before.

When the destination node receives the packet containing the route request, it replies by sending a route that was saved in the request packet. If a source node does not receive any reply after a specified amount of time, it sends another route request.

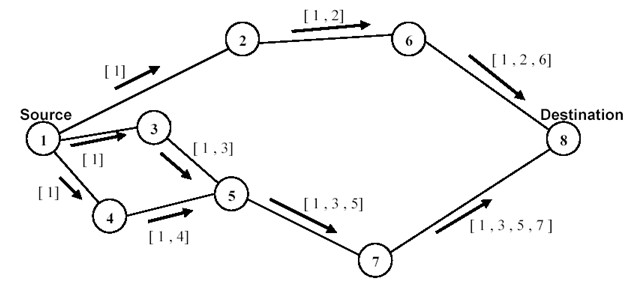
When data is being routed in CBRP, if a node senses that a link is broken, it sends an error message to the source node, and then it begins using a local restitution process. In this process, if a given node N finds that a next node M cannot be reached, N tries to verify whether M or the node after it can be reached through a neighboring node. If one of these cases is verified, data is sent using the newly restituted route.[2]

## Dynamic Source Routing (DSR):

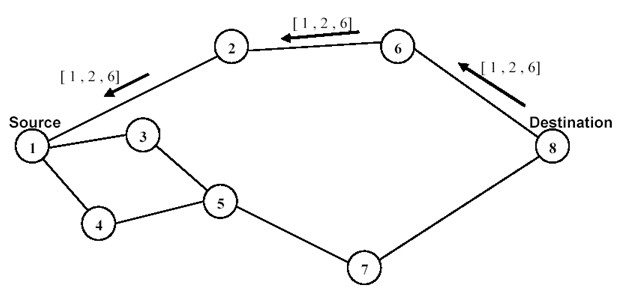
DSR (Dynamic Source Routing) [14] is a reactive protocol.it uses a technique known as "Source Routing" in which the transmitter (source) indicates the complete route by which a packet must pass to reach its destination, this route is inserted in the header of the packet. The intermediate nodes between the source node and the destination node need not maintain the information on the traversed route since the complete route is inserted in the header of the packet.

If a node in DSR wants to communicate with a destination it does not own no route, it floods the network with a query packet (RREQ) similar to that of AODV.

Each node that receives the request and does not have a route to the requested destination inserts its address into the RREQ packet and distributes it to its neighbors.

The response to the request (RREP) is returned by the destination or by another node that has a route to the destination.

## Figure I.8 building record route during route discovery [15]



**Figure I.9 propagation of route reply with route record [15]**

* + - 1. **Advantages of reactive protocols**
* Saving network resources: No control messages load the network for unused paths.
* It requires minimum of routing information.
* Overhead is small which results in a low bandwidth use in the networks.[5]

## Disadvantages of reactive protocols

* Network overload when requesting routes.
* Longer wait times.
* The installation of a path by flood can be costly.[4]

## Hybrid routing protocols

Hybrid protocols combine the two ideas: proactive protocols and reactive protocols. They use a proactive protocol to get information about the nearest neighbors (maximum neighbors with two jumps).

Beyond this predefined area, the hybrid protocol uses reactive protocols to search for paths. With this division, the network is split into several zones, and path searching in reactive mode can be improved.

This type of protocol adapts well to large networks. However, it cumulates the disadvantages of reactive and proactive protocols at the same time.[17]

## Zone Routing Protocol (ZRP):

The ZRP routing protocol uses both approaches (Proactive and Reactive), it limits the proactive procedure only to nodes neighbors (changes in topology must have a local impact) and, nature comprehensive, offers a fast and efficient search in the network. Unlike a network-wide search, in this protocol, detection of routing loops is possible thanks to knowledge of the network topology.

An intra-zone routing is defined for each node, including the nodes which are at a minimum distance (in terms of number of hops), of the node in question, less than or equal to the radius δ of the zone.

In summary, ZRP therefore defines two types of protocols: one operating Locally and the second operating between zones. These two protocols are:

* IARP (Intrazone Routing Protocol) offering optimal routes to

Destinations within the zone at a specified distance, and any changes are reflected only within the area.

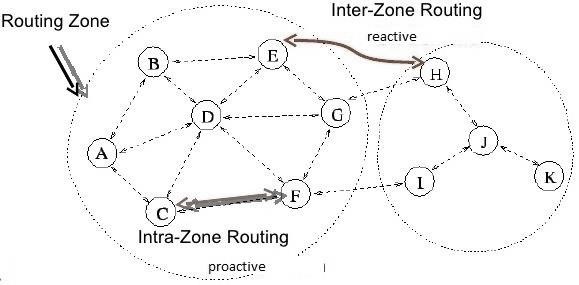
* IERP (Interzone Routing Protocol) is responsible for Routes to destinations outside of an area.

In addition to these two protocols, the ZRP uses the BRP protocol (Bordercast Routing

protocol), this protocol uses the topology data provided by the IARP protocol to build its list of nodes. It is used to guide the propagation of search queries from The IERP in the network. The path search is performed by first checking if the destination node is not in the source node area (the IERP procedure assumes that each node knows the contents of its zone), in which case the path is already known.

Otherwise, a "RREQ" route request is initiated to all the peripheral nodes, the latter verifying, in turn, whether the destination specified by the source exists in their zones. In the positive case, the source will receive then a packet "RREP" containing the path leading to the destination, otherwise the nodes broadcast the request to their own peripheral nodes, which in turn perform the same processing.

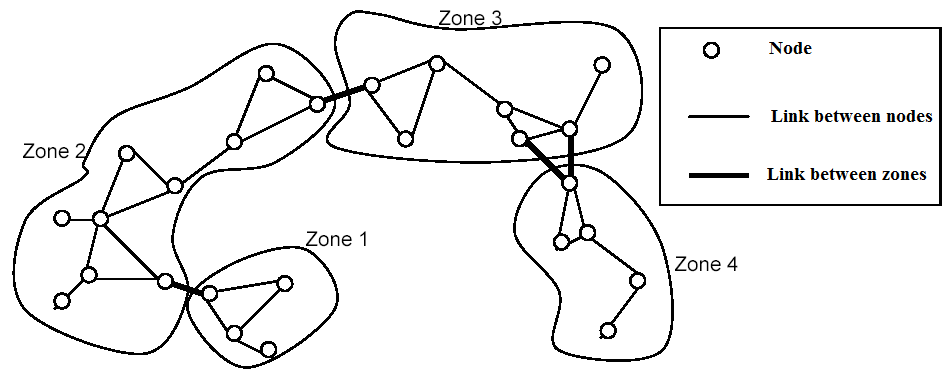
Route errors are also provided by the IERP using a reactive response mechanism. When a packet is propagated, if an error occurs at the next node (the node becomes inaccessible), a "RERR" message is delivered to the source.[15]



## Figure I.11 Zone Routing Protocol [15]

* + - 1. **Zone Based Hierarchical Link State Routing Protocol (ZHLS):**

The zone based hierarchical link state routing protocol (ZHLS) is based on the technique of dividing the network into a collection of zones. However, unlike other hierarchical protocols, members of a particular zone do not select a representative, or head. The decomposition in ZHLS results in two topology levels: the zone level, and the node level. A topology that is based on the node level describes the way in which a zone’s nodes are physically connected. A virtual link can exist and be established between two zones if there is at least one node in the first zone that is physically connected to another node in the second zone.

The zone level emits the layout, or outline, of the links and connections between different zones.[17]

## FigureI.10: dividing the network into zones by ZHLS protocol.[17]

In ZHLS, packets that contain links or LSPs (Link State Packets) can be divided into two distinguished classes: node oriented LSPs, and zone oriented LSPs. For any given node, a node oriented LSP packet comprises the information of a neighboring node, whereas a zone oriented LSP packet contains the information about the zone. In this manner, every node of the network possesses a complete knowledge regarding nodes in its own zone, and only partial knowledge regarding the rest of the nodes.

The aforementioned partial knowledge is materialized by the state of the connection between the different zones in the network. Thus, data routing can be achieved in one of two ways: inter zone routing, or intra zone routing. (Meaning the use of inter zone routing tables and intra zone routing tables is involved).

For any given destination, data packets are sent between zones by using the zones’ identifiers (IDs), which continues until the data packets reach the final zone of the destination. Follow that, data packets move around the final zone and navigate using the destination node’s identifier (ID). The address <Zone ID, Node ID> is amply sufficient to reach any given destination, no matter the changes that occur to the network.[15]

# Security in mobile ad hoc network:

The Ad-Hoc mobile networks are considered very weak in terms of attacks of all kinds. When a station sends data, any unit equipped with a listening device (here Wi-Fi cards) has the possibility of intercepting this data. Hackers can therefore intercept data in a direct way by using pirate antennas (because the data circulate by radio) or oblige a station to consume a large part of its energy resources by flooding it with all kinds of unnecessary requests.

The lack of central management of network functionality makes these networks much more vulnerable to attacks than wireless (WLAN) and (LAN) networks.[7]

## Possible Attacks in Routing Protocols:

In this section, we list possible attacks that target routing protocols. This type of attack can disrupt the operation of the network.

These attacks can also be classified into two categories:[16]

## Deleting packet attacks:

In this type of attack, the intruder removes all or some packets. We can find two types:

* Black holes: The attacker removes all packets (control and data).
* Gray holes: This is a particular case of the black hole in which the attacker deletes the data

packets and transmits the control packets.

## Attacks by Changing Routing Information:

In the absence of integrity check on the transmitted messages, a malicious node may redirect traffic to it or cause a denial of service, simply by changing some of the control packets used by the routing protocols.

According to the modified field, the attacks can be classified as follows:[18]

* **Redirect by changing the sequence number:** Some protocols for routing like AODV use a sequence number associated with the destination that indicates the freshness of the route. A malicious node can therefore modify the value of the sequence number field to divert traffic to it. Then, it can intercept, delete or modify this traffic.
* **Redirection by changing the hop count:** The protocols routing to distance vector as AODV use a field called hop count that indicates the length of the route. To establish a communication with another node, the source chooses the route with the lowest hop value. Thus, a malicious node can divert traffic to it by announcing at the source a route having a smaller hop count.
* **Denial of Service by Changing Routing Information by source routing:** The DSR protocol explicitly indicates the different nodes of the route in the header of the data packet. A malicious node can cause routing loops or throw a denial of service by changing the list of nodes indicated in the packet.

## Spoofing Attack:

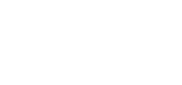
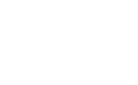
In this attack the adversary assumes the identity of another node in the network by modifying either the IP or MAC address in outgoing packets in order to appear as legitimate node and to establish a connection that will allow him to gain access to the other hosts and their sensitive data.[16]

# I.6 conclusion

This chapter presents mobile ad hoc networks, their characteristics and applications. They are distinguished from other networks by their great flexibility of use and their high robustness but also by additional constraints such as energy limitation and lack of central element to manage the network. We also presented the routing problem that is most important in this type of network, and the difficulties posed by the mobility of the nodes.

Proposed protocols are classified into two main categories: proactive protocols and reactive protocols. The protocols of the two categories try to adapt to the constraints imposed by the ad hoc networks, by proposing a method which is of lower resource cost. And which guarantees the survivability of the routing in case of links or nodes breakdown.

The design of a routing protocol for ad hoc networks must take into account all physical factors and limitations imposed by the environment so that the routing strategy does not degrade the performance of the system.



# Introduction:

When transmitting a packet from a source to a destination, it is necessary to use a routing protocol that will route the packet correctly through the "best" path. Several protocols have been proposed at the ad hoc level. In order to understand their behavior in mobile networks, we were interested in doing a theoretical study on the reactive protocol AODV.

Indeed, this protocol shows a better qualification. AODV is representative of various techniques and is the most advanced on the way to standardization. It belongs to a family of reactive protocols. It uses a broadcast mechanism in the network to discover valid routes.

We will present this protocol, starting with a detailed study on the AODV routing protocol and how it works.

# Definition of AODV:

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol used in MANETs (Mobile Ad hoc Networks) that reduces number of broadcast by creating routes on demand basis. AODV routing mechanism is based on two approaches, route discovery and route maintenance. This protocol uses the principle of sequence numbers to maintain the consistency of the routing information. Due to the mobility of the nodes in the ad hoc networks, the roads change frequently so that the roads maintained by certain nodes become invalid. Sequence numbers allow you to use the newest routes, in other words, the freshest route.[2]

The AODV uses a route request in order to create a path to a certain destination. However, the AODV maintains the paths in a distributed manner by keeping a routing table at each transit node belonging to the searched path.

AODV does not update routes regularly, instead the routes are discovered and maintained if it’s required. It uses three types of messages for routing, RREQ to request a route, RREP to reply to a route request and RERR to signal a route breaking (error). [19]

# Characteristics:

* + - Uses bi-directional links.
    - Route discovery mechanism used for route finding.
    - Maintenance of active routes.
    - Sequence numbers used for loop prevention and as route freshness criteria.
    - Provides unicast and multicast communication.
    - Minimizes number of active routes between an active source and destination.
    - Can determine multiple routes between a source and a destination, but implements only a single one.
    - AODV discovers routes as and when necessary. (Does not discover routes to and fro every node).
    - Routes are maintained just as long as necessary.
    - Every node maintains its monotonically increasing sequence number.[12]

# Terminology of AODV:

## Active (or valid) route:

An active route is one whose routing table entry is marked as valid. Only active routes can be used to forward data packets, inaccessible entries are then deleted.

## Broadcast:

Broadcasting is transmitting to the IP Limited Broadcast address “255.255.255.255” A broadcast packet may not be blindly furthered, but broadcasting is used to enable the distribution of AODV messages throughout the ad hoc network.

## Forwarding node:

An intermediate node that will forward packets destined for another node, by retransmitting them to a next hop that is closer to the destination.

## Forward route:

A route set up to send data packets from a node initiating a route discovery process towards its desired destination.

## Invalid route:

A route that has expired, represented by a state of invalid in the routing table entry. An invalid route is used to store previously valid route information for an extended period of time. An invalid route cannot be used to forward data packets, but it can provide information useful for route maintenance, and also for future RREQ messages.

## Reverse route:

A route set up to forward a route reply packet (RREP) back to the source from the destination or from an intermediate node having a route to the destination.

## Sequence number:

The Sequence number is used to distinguish between old and new routes, which avoids the formation of routing loops.[23]

# Routing Table:

The AODV uses a route request in order to create a path to a certain destination. However, the AODV maintains the paths in a distributed manner by keeping a routing table at each transit node belonging to the required path. Road information should be retained even for short duration routes. The structure of this table is presented in the following figure.[15]

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| @Des | #SN | Valid-SN | State | Interface | #HC | @NH | PL | LT |
|  |  |  |  |  |  |  |  |  |

## Figure II.1 Routing Table Format [2]

* @D: destination IP address.
* #SN: Sequence Number of destination.
* Valid\_SN: Flag indicating the validity of the sequence number.
* State: Flag indicating the entry state (for example: Valid, Invalid, repairable).
* Interface: Network Interface.
* #HC (Hop Count): number of hop counts necessary to reach the destination.
* @NH (Next Hop): next hop towards the destination.
* PL (Precursor List): list of neighbors where response generated or transferred.
* LT (Life Time): Time beyond which the route expires or is deleted.

# Messages Format:

* + 1. **Route Request (RREQ):** This message is broadcast when a node determines that it needs a route to a destination and does not have an available route. This is the case when the destination is unknown or when a previously valid route in its routing table expires or is



marked invalid. The node created the packet shown in Figure II.2 [21]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Type | J | R | G | D | U | Reserved | Hop count |
| RREQ identifier | | | | | | | |
| Destination IP address | | | | | | | |
| Destination sequence number | | | | | | | |
| Source IP address | | | | | | | |
| Source sequence number | | | | | | | |

## Figure II.2 RREQ Packet Format [21]

* Type (8 bits): this field indicate the packet
* Flags (5 bits): this field contain five flags (J, R, G, D, U) such as:
  + J: Join flag, used for multicast.
  + R: Repair flag, reserved for multicast.
  + G: Gratuitous RREP flag: Indicates the need to generate a route response to the destination in addition to that generated to the source to inform it that such a source is seeking to join it and thus a bidirectional path is established. An RREP of this kind (free) is generated only when it is an intermediate node that responds.
  + D: Destination only flag: indicate that only the destination can respond to this route request.
  + U: Unknown Sequence Number: indicate that the sequence number of destination is unknown.
* Reserved: Set to zero at sending and ignored on reception.
* Hop Count: The number of hops from the source to the node initiating the request.
* RREQ ID: A sequence number uniquely identifying a route request when associated with the address of the source.
* Destination IP address: IP address of the destination to which a route is requested.
* Destination sequence number: last sequence number known for destination
* Source IP address: IP address of the node that initiate the route request.
* Source sequence number: Current sequence number of the source that will be associated with the input of the routing table in the nodes processing the RREQ message.
  + 1. **Route Reply (RREP):** When a route request reaches the destination or a node with a valid path to the destination, it generates a route response that will be sent in unicast from one node to another until the source is reached. The route response packet is represented by Figure

II.3 [21]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type | R | A | Reserved | Prefix sz | Hop count |
| RREQ identifier | | | | | |
| Destination IP address | | | | | |
| Destination sequence number | | | | | |

|  |
| --- |
| Source IP address |
| Life Time |

## Figure II.3 route reply packet [21]

* Type (8 bits): this field indicate the packet type.
* Flags (2 bits): this field contain two flags:
  + R: Repair flag, used for multicast.
  + A: Acknowledgment of receipt required.
* Reserved (9 bits): Set to zero at sending and ignored on receipt.
* Prefix Sz (5 bits): If it is non-zero, this means that the next hop can be used for any node with the same prefix.
* Hop Count (8 bits): Number of hops from the RREQ destination to the node currently being treated.
* Hop Count: The number of hops from the source to the node initiating the request.
* Destination IP address: IP address of the destination to which a route is requested.
* Destination sequence number: last sequence number known for destination
* Source IP address: IP address of the node that initiate the route request.
* Lifetime (ms): Time for which the nodes receiving the RREP consider the route as valid.

**II.6.3 Route Error (RERR):** A route error is sent whenever the disruption of a link makes access to one or more destinations impossible.[21]



|  |  |  |  |
| --- | --- | --- | --- |
| Type | N | Reserved | Dest count |
| Unreachable Destination IP Address | | | |
| Unreachable Destination Sequence Number | | | |
| Additional Unreachable Destination IP Addresses | | | |
| Additional Unreachable Destination Sequence Numbers | | | |

## Figure II.4 route error packet

* Type (8 bits): the value of this field takes 3 in RERR message.
* Flag (l bits): it contains one flag, N (No delete flag) Set to one when the node performs a local repair of the route and the upstream nodes must not clear the route..
* Reserved (5 bits): Set to zero at sending and ignored on receipt.
* Destination Count (8 bits): The number of non-reachable destinations included in the message. This value must be at least 1.
* Unreachable Destination IP address: The IP address of the destination that is no longer accessible.
* Unreachable Destination Sequence Number: The sequence number of the destination (taken from the routing table) which the IP address is just above.

# II.7 AODV Functioning:

AODV is a reactive routing protocol that based on two mechanisms: route discovery and route maintenance.

## Route discovery:

When a node needs to send a message, it looks in its routing table if a valid route exists for the destination it wants to reach or not, if it does not exist, it initiate a search of a route. This task is performed by broadcasting RREQ messages over a broadcast address over a network, as shown in figure II.5.



S



D

RREQ

## Figure II.5 Propagation of RREQ [2]

The RREQ packet destination sequence number field contains the last known value of the sequence number associated with the destination node. This value is copied from the routing table, if the sequence number is not known, the null value will be taken by default. Before sending the RREQ packet, the origin node saves the message identifier (RREQ ID) and the IP address so that it does not process the message in case a neighbor returns it. After the route request is made, the requesting node puts itself on hold.[20]

When a transit node (intermediate) receives the packet of the request, it verifies in its history table if this request has already been treated and processed. If the packet is duplicated, the node must ignore it and stop processing. Otherwise the pair (@ source, RREQ ID) will be

entered in the history table to reject the future duplicates, and the node continues the processing by looking for the destination in its routing table: if it has a recent route, Note that a route is recent if the sequence number of the destination in the table is greater than or equal to the sequence number in the RREQ packet. In this case, the node sends a response packet (RREP) to the source indicating how to reach the destination as shown in figure II.6.



S D

RREP

## Figure II.6 propagation of RREP [2]

Otherwise the node does not know the route to the destination: it increments the number of hops and rebroadcasts the packet.

Before sending the packet, the intermediate node saves the address of the previous node and that of the source node from which the first copy of the request is received. This information is used to construct the inverse path, which will be traversed by the unicast route response packet (this means that AODV only supports symmetric links).

If the query reaches the destination node, a RREP packet is constructed with the new sequence number of the destination and followed the reverse route noted in the table (see Figure II.5). The hop count field of RREP route message is incremented at each traversed node, once the origin node has been reached, the value of the hop count field represents the distance in number of hops to go from the source node to the destination node.[8]

When the node receives a route response, the packet is examined and an entry for the route to the destination is written to the routing table if at least one of these conditions is satisfied:

* No route to the destination is known.
* The sequence number for the destination in the response packet is greater than the value present in the routing table.
* The sequence numbers are equal but the new route is shorter.

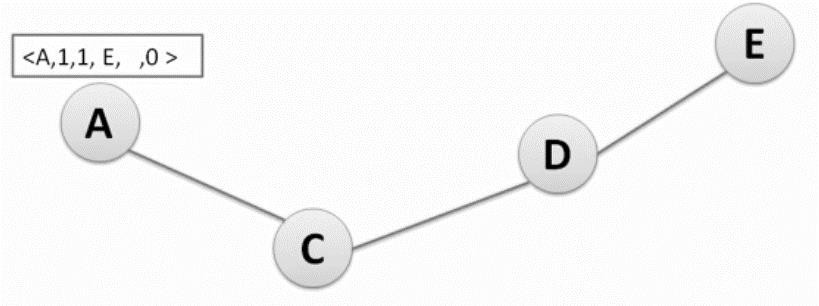
In order to limit the cost in the network, AODV proposes to extend the search progressively,

initially, the request RREQ is broadcast to a limited number of hops. If the source does not receive a response after a specified timeout called RREP\_WAIT\_TIME, it rebroadcast another request by increasing the maximum number of hops. In case of non-response, this procedure is repeated a maximum number of times before declaring that this destination is unreachable.

For each new broadcast, the RREQ ID field of the RREQ packet is incremented to identify a particular route request associated with a source address. If the RREQ request is re-broadcast a certain number of times (RREQ.RETRIES) without receiving a response, an error message is triggered.[2]

## Illustration of route establishment in AODV Step 1:

* + - * Node A needs a routing path to node E.
      * Node A creates a RREQ packet.
      * RREQ [A’s IP addr, src seq#,Broadcast ID, E’s IP addr, dest seq#, hopcount]
      * Node A broadcasts RREQ to its neighbors.



## Figure II.7 initiating route discovery [24]

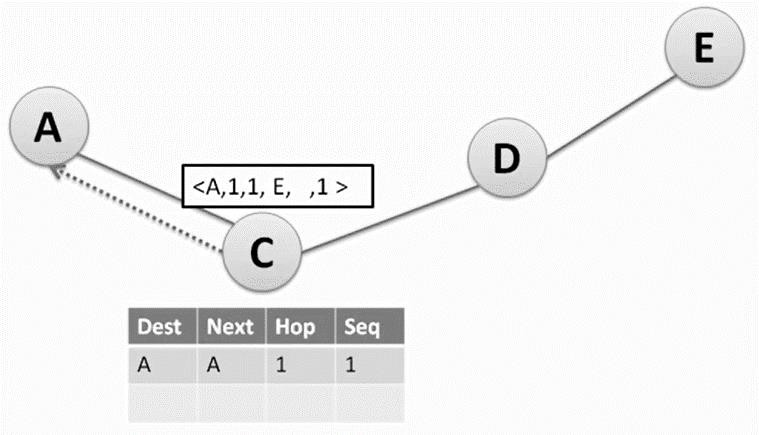
**Step 2:**

C increase hop count in RREQ.

C check its routing table if it has a valid route to E. C check its routing table and finds nothing.

C record the address of the node from which it receives the first RREQ packet (A), to use it for reverse path.

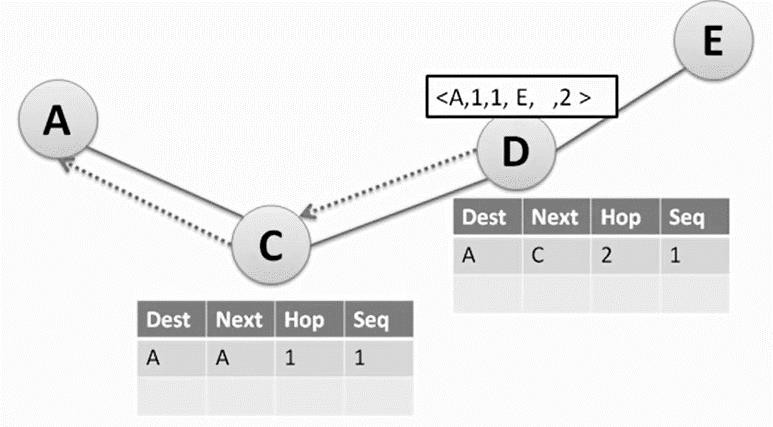
C rebroadcast RREQ to its neighbor (D).



## Figure II.8 broadcast RREQ to C [24]

**Step 3:**

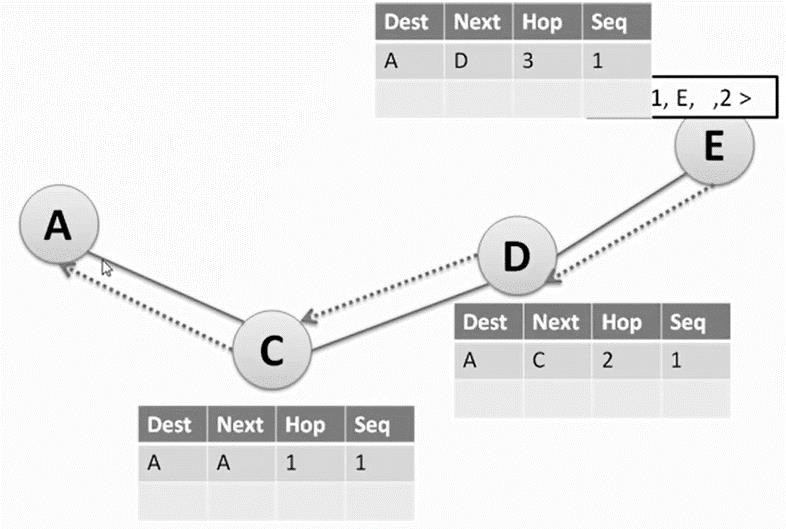
* + - * D increase hop count in RREQ.
      * D check its routing table if it has a valid route to E.
      * D check its routing table and finds nothing.
      * D record the address of the node from which it receives the first RREQ packet (A), to use it for reverse path.
      * D rebroadcast RREQ to its neighbor (E).



## Figure II.9 broadcast RREQ to D [24]

## Step 4:

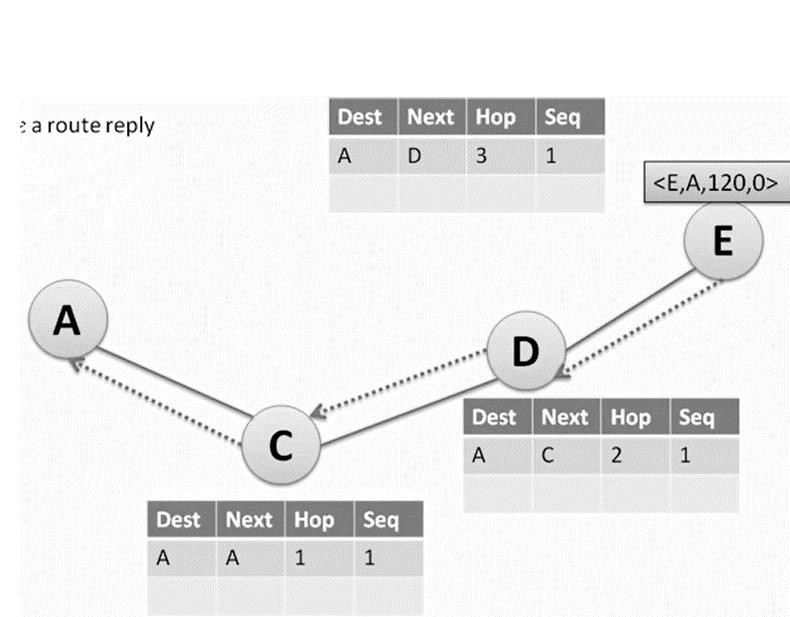
* + - * The RREQ reach the destination node E with Hop count = 3.
      * E record the address of the node from which it receives the first RREQ packet (A), to use it for reverse path.



## Figure II.10 broadcast RREQ to E [24]

**Step 5:**

* + - * E creates a route reply (RREP) and unicast the RREP to D.
      * RREP [E’s IP addr, A’s IP addr, dest seq#, hopcount].



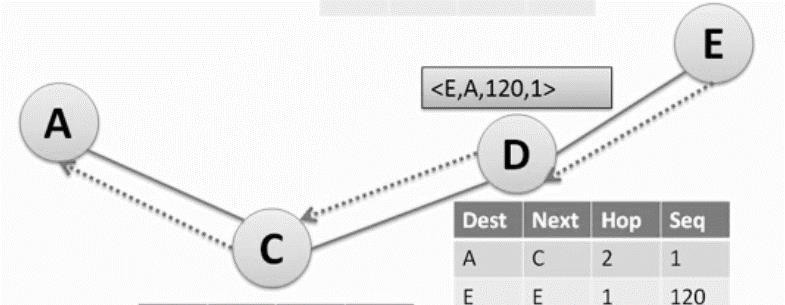
## Figure II.11 destination node E creates a RREP [24]

**Step 6:**

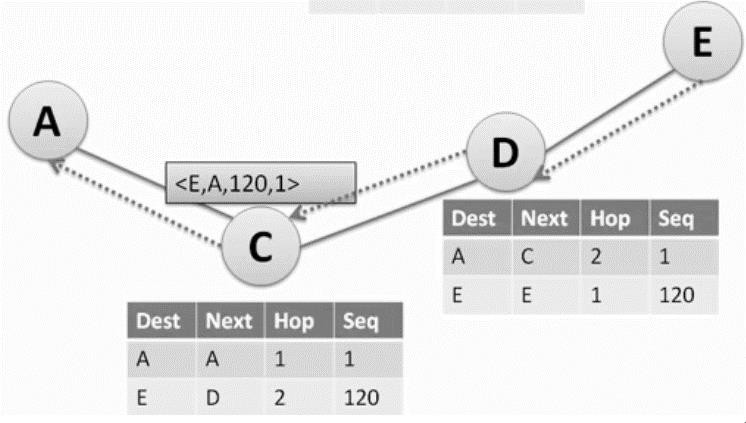
* + - * Fig: - D will create an entry for node E in its routing table to use it for forward path.

- D increase hop count in RREP.

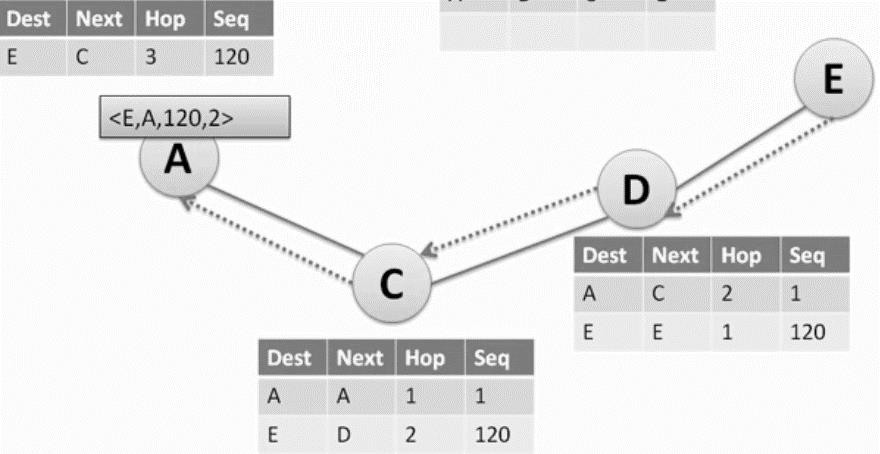
* + - * Fig: Also, C create an entry for node E in its routing table and increase hop count.
      * Fig: then, A create an entry for node E in its routing table and increase hop count.



## Figure II.12 destination node E unicast RREP to D [24]



**Figure II.13 node D unicast RREP to C [24]**



**Figure II.14 node C unicast RREP to source node A [24]**

**Step 7:**

* + - * The RREP reach the source node A.
      * Source node A can forward data packet to destination.

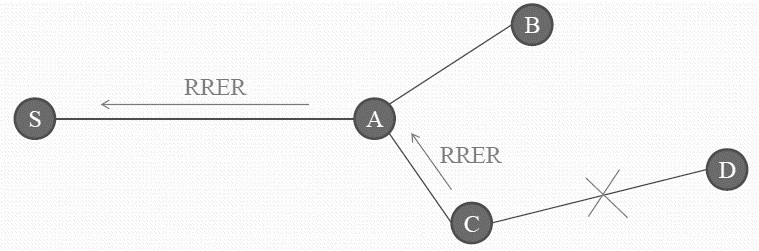
## Route maintenance:

AODV maintains routes as long as they are active, a route is considered active as long as data packets transit periodically from source to destination along that path. If a link breaks the entire active route, the link is considered faulty. The failures of the links are, in general, the duties to the mobility of the ad hoc network.

In order to detect this failure, AODV uses the "HELLO " control messages to verify the connectivity or rather the activity of the roads. A node determines the connectivity of a route by periodically listening to the "HELLO" messages transmitted by its neighbors. If, for a period of time, three HELLO messages are not received consecutively, the node considers that the link to this neighbor is broken. It sends an error message (RERR) to the source and the route becomes invalid. [8]

## Illustration of route maintenance in AODV:

* Assume link between C and D breaks.
* Node C invalidates route to D in route table.
* Node C creates RRER packet and sends to its upstream neighbors.
* Node A sends RRER to S.
* Node S rediscovers route if still needed.



## Figure II.15 route maintenance [24]

* 1. **Advantages of AODV:**
     + AODV minimizes the number of broadcasts messages because it discovers a route on demand.
     + AODV can respond very quickly to the topological changes that affect the active routes, because of its adaptability to highly dynamic networks.
     + During inoperativeness, AODV has the ability to save bandwidth and energy.
     + AODV can handle and work for tens of thousands of mobile nodes.
     + AODV can perform local repairs, and alows for a node’s parameters to be configured per requirement.
     + AODV is compatible over wired and wireless networks.
     + It has a lower setup delay for connections and detection of latest route to the destination.[23]

# Disadvantages of AODV:

* + - This protocol has a high processing demand.
    - It takes long time to build the routing table.
    - A large number of control packets are generated when a link breakage occurs. These control packets increase the congestion in the active route.
    - High route discovery latency, that can be high in large-scale networks because AODV discover route only on demand.
    - AODV consumes a large share of bandwidth.
    - A size the network grows, various performance metrics begin decreasing.[19]

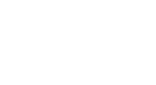
# II.6 Security vulnerabilities of AODV:

AODV is vulnerable to routing attacks by malicious nodes due to the lack of security features. While the on-demand property of AODV enables its advantages on low protocol overhead and adaptability to host movement, it is susceptible to many types of attacks:

1. Modifying or forging RREQ or RREP packets.
2. Deceiving destination or source IP address to act as a genuine network node and thus receiving or dropping data packets.
3. Generatinging fake RERR packets to increase routing delay and impair network performance.
4. Causing DoS by sending fake RREPs of highest sequence numbers (Blackhole attack).
5. Creating routing loops and launching sleep deprivation or resource consumption attacks to deplete node batteries.
6. Replaying old routing messages or making a tunnel/wormhole to disrupt the normal routing behavior.[18]

# Conclusion:

The AODV routing protocol does not ensure the use of the best path between source and destination. However, recent performance evaluations have shown that there are no great differences (in terms of optimization) between the paths used by the AODV protocol and those used by the protocols based on the shorter path algorithms. In addition, the AODV protocol does not have a routing loop and avoids the counting to infinity problem of Bellman-Ford, which offers rapid convergence when the topology of the ad hoc network changes.



# introduction:

Simulation is currently the most practical tool to evaluate the behavior of a complex system whose formalization using analytical methods is difficult. To test the performance of a mobile network, simulation is often used. Indeed, it would be too costly, if not impossible, to set up a network for testing purposes for certain criteria. For example, testing applications on large networks is only possible if material resources are available. However, in the context of a simulation, it is sufficient to change the simulation parameters corresponding to the size of the network.

A simulation on wireless networks that does not take very long much time that brings us closer to the actual use of the routing protocol. These advantages Help us select the best protocols that have good behavior in Different scenarios. The protocol developers also do Simulation to improve the capabilities of their routing algorithm.

# definition of simulation:

To simulate is to model a complex system, in order to predict its behavior in the real world. It is an approach to represent the functioning of a real system consisting of several entities, to model the different interactions between them, and finally to evaluate the overall behavior of the system and its evolution over time.

The use of simulation allows to limit the complexity of the analytical models. However, it is necessary to clearly identify the characteristics of the system in order to represent it, as finely as possible, by abstract models. If the representation of the real system by abstract models is sufficiently realistic and precise, it is then possible to transfer the results obtained with these models to the real system.[25]

## cases of simulation:

The simulation of a real system becomes necessary when the analytical models become either too complex in terms of calculation and resolution time, or too simplified with respect to the reality, thereby making the results obtained not representative of the behavior of the system in a real environment. Thus, simulation may be necessary in the following cases: [27]

* + - * The system is not decomposable into simple subsystems independent of each other, making analytical modeling very complex.
      * The system does not yet exist. In this case, the simulation can constitute a preliminary phase, allowing the designers to predict the operation of the system in order to optimize the dimensioning of its various parameters.
      * Experiments on real systems are too costly in terms of material and human resources.
      * Experiments on real systems are not reproducible nor representative of all possible environments. In this case, the simulation allows to characterize the global behavior of the system for different environments

## Types of simulations:

There are five main types of simulations: [26]

* + - * **Stochastic simulations:** The input and output variables are random with certain probabilities.
      * **Dynamic simulations:** These simulations are specialized for systems that change as time progresses.
      * **Static simulations:** Contrary to the dynamic ones, these simulations can only be applicable if no changes of the system occur in time, or if time does not have any effect on the studied entity.
      * **Deterministic simulations:** contrasting with stochastic simulations, deterministic simulations have specific variables as input, and they have expected results. They are usually used to define the essential mechanics or behavior of a phenomenon, process, or mechanism.
      * **Discrete event simulations:** This type of simulations allows for the modeling of a real system whose behavior can change with the addition or apparition of phenomena or events with the progress of time.

## Advantages and disadvantages of simulations: Advantages:

* + - * Allows the critical observation of a giver system’s states.
      * Allows the study of a system or entity without being constricted with materiel limitations.
      * Analyzing the impact of variables on the performance of a studied system.
      * Studying the main functioning points of a system.[27]

## Disadvantages:

* + - * Conceiving and creating models can demand a certain level of expertise and experience.
      * Results can vary in authenticity and are not necessarily all applicable and generalized.[25]

# Modeling:

## Definition:

Modeling is a technique that aims for the representation of a system, a physical object, or mathematical logic. It essentially simplifies the intended work by eliminating all the details that are deemed too difficult to reproduce, and all the while focusing solely on the important traits of the modeled entity. This helps acquire a more polished result. In the context of computer simulations for example, a model is the assembly of specific algorithms, equations, and data used to encompass and pinpoint the behavior and conduct of a studied entity, while a simulation is the running and applying of all that data. Essentially, we build a model then run a simulation based on that model. [32]

As a discipline, modeling has its own set of rules and regulations, depending on which field is being studied or researched:

-A model represents a reality, but it does not constitute that reality. It is the same logic that applies in the making of maps. Maps are a representation of real geography, but they do not constitute the territory. [33]

-A model is not, and does not have to be, perfectly similar to the studied entity. The level of resemblance varies depending on the desired utilization. In that effect, a doctor and an artist do not use the same model for the human anatomy. [33]

-The quality of the model is reliant on the techniques and technologies used. Its behavior is only similar to that of the studied entity on a specific level. Therefore it is quantifiable and based on the desired use of the model. [32]

## Pre-requirements of modeling:

There are pre-requirements that must be established before initiation modeling:[29]

* + - * **The purpose of the modeling:** There must be a specific goal for the modeling.

Example: A representation of a biological phenomenon, a network simulation…etc.

* + - * **The model’s complexity level:** Since there are models that require a deep understanding and knowledge of the case study, while others can automatically be used by a computer or a program, it is imperative that the user acknowledges the complexity of the model intended, as well as the ability to manipulate and manage it.
      * **The model’s precision:** The precision desired of the model must be established, because it is a characteristic that varies from one model to another. Example: a weather forecast model does not have, or require, the same precision than that of a real-time plane control model.

## Types of models:

Models, upon which modeling and simulation rely on, have a myriad of variations and categories, which are contingent on the field of study:

* + - * **Economic models:** In economy, a model is simplified representation of an economic reality, or process, or a part of either. Economic models often use mathematical formalism to represent the model in equations, variables, or diagrams.

Economic models are very useful, as they help establish previsions of the market’s

behavior and status, and also improve economic situations.

Example: The Solow–Swan model of economic growth, Gordon-Loeb’s model of information security investment…etc. [34]

* + - * **3D models:** They are three-dimensional representations of physical objects using geometrical shapes and connected points across three-dimensional space. They can be created by hand, algorithmically, or by scanning real-world objects. 3D objects can be represented in one of three ways: polygonal, curve modeling, and digital sculpting. 3D models are used in a myriad of fields, most notable medicine, architecture, gaming, animation and filmmaking…etc. [34]
      * **Mathematical models:** A mathematical model is a translation of an observation to apply tools, techniques, and mathematical theories on it. It can also be the translation of mathematical results obtained via predictions or operations made in the real world. It is primarily used in chemistry, physics, agronomy…etc. [34]
      * **Computer models:** They are models that are created for the purpose of computer simulations and can represent objects or systems. They are what computer simulations depend on to function and run.

Computer models can be classified according to several independent pairs of attributes, including:

-Stochastic or deterministic. (Based on the type of process that is simulated).

-Steady-state or dynamic.

-Continuous or discrete.

-Dynamic system simulation.

-Local or distributed. [1]

## Calibration, verification, and validation of models:

In order to correctly portray theoretical scenarios by simulations, accurate simulation models must be created and used. Models have to match what is currently happening in real. To that end, three steps must be followed:[33]

## Calibration:

Model calibration is the process of adjusting and fine-tuning any and all available settings and parameters to control how the model functions. This will ensure that the simulation using the model matches the characteristics of the area, or case study, that is being studied.

## Verification:

Model verification is the technique that ensures that the obtained output data from the model matches the calculated results that are expected from the input data.

## Validation:

Validation is the final step, and it involves comparing obtained results from the model with the historical results expected in that specific field of study. If model outputs differ greatly from what is historically expected, then it may be that the model contains errors.

## Applications of simulation models:

Simulation models are found to be useful in many fields, and new applications are discovered almost daily. Following are the main axes that simulation models can be used in:

-Scientific comprehension.

-Technological system development.

-System organization.

-Development projection. [29]

# Definition of network simulation:

Network simulation is a valuable technique since the comportment of a network can be modeled by calculating the communication between the different network constituents (they can be end-hosts or network units such as routers, physical links or packets) using mathematical formulas. They can also be modeled by actually or virtually capturing and playing back experimental observations from a real production network. After we get the observation data from simulation experiments, the behavior of the network and protocols supported can then be observed and analyzed in a series of offline test experiments. All kinds of environmental attributes can also be modified in a controlled manner to assess how the network can behave under different parameters combinations or different configuration conditions. Another characteristic of network simulation that worth noticing is that the

simulation program can be used together with different applications and services in order to observe end-to-end or other point-to-point performance in the networks.[25]

# Network Simulators:

* + - **NS2:** is the most popular simulator for modeling wired and wireless networks. NS2 is developed in C ++ and uses the OTcl language to write scripts and configuration files. Since the popularity of this tool, several simulation models have been developed and are currently available: MAC layer (CSMA, CDMA, MPLS, etc.), network layer (IP, AODV, DSR, and UDP), etc.[35]
    - **Ns3:** is an open sourced discrete-event network simulator, targeted primarily for research and educational use. Ns-3 is a free software, licensed under the [GNU GPLv2](http://www.gnu.org/copyleft/gpl.html) [license.](http://www.gnu.org/copyleft/gpl.html)

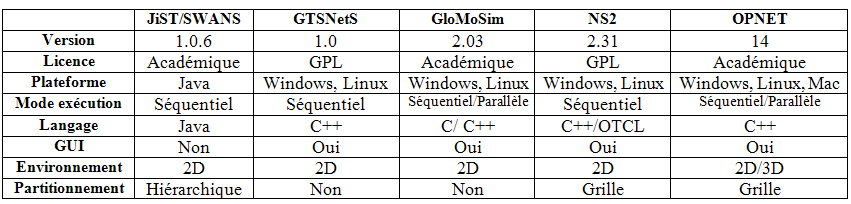
Ns3 aims to develop a preferred, open simulation environment for networking research and development: it should be aligned with the simulation needs of modern networking research.NS3 is designed to replace the current popular NS2. However, NS3 is not an updated version of NS2 since NS3 is a new simulator and it is not backward-compatible with NS2. [35]

* + - **OMNet ++ :** is a discrete event simulator based on the C ++ language, designed primarily to simulate network protocols and distributed systems. It is fully programmable, configurable and modular. It is an open source application under the GNU license, developed by Andras Varga, researcher at the University of Budapest.[36]

**OPNET:** is very large and powerful software with wide variety of possibilities, enables the possibility to simulate entire heterogeneous networks with various protocols.Originally the software was developed for the needs of military, but it has grown to be a world leading commercial network simulation tool.

OPNET is quite expensive for commercial usage but there are also free licenses for educational purposes.[26]

* + - **GloMoSim:** is a simulation environment written in Parsec. This language allows the implementation of sequential simulation and parallel to discrete random. Thanks to the parallelism, GloMoSim is able to simulate networks consisting of several tens of thousands of nodes. Several simulation models have been implemented within this simulator.[28]
    - **JiST / SWANS:** is a discrete event simulator written in Java. This simulator relies on Jist, a generalist engine allowing the implementation of simulators with discrete events. This engine runs on top of the Java virtual machine and it has been shown to be more efficient than NS2 and GloMoSim in terms of memory usage and speed of execution.[29]
    - **GTSNeTS** (Georgia Tech Sensor Network Simulator) is a simulator written in C ++ and dedicated to the simulation of wireless sensor networks. This simulator is capable of simulating several hundreds of thousands of nodes. However, the biggest disadvantage of this simulator is the lack of realistic modeling of the physical



layer.[34]

# Opnet Modeler:

## Figure III.1 network simulators[36]

* + 1. **Definition:** OPNET (Optimum Network Performance) is a very powerful and comprehensive network simulation tool. Based on an intuitive graphical interface allows to draw and study communication networks, equipment, protocols and applications with ease and scalability. Modeler is used by leading technology companies, researchers, engineers, universities and even the US military to accelerate their research and development processes. The object-oriented approach, as well as the debugging and analysis features associated with Modeler’s embedded graphical editors simplify the composition of networks and equipment, which in turn makes it easy to match your information system to your model.

Modeler has a user-friendly graphical interface, is based on a series of hierarchical editors that parallelize the actual network structure, equipment is protocols.[26]

## Opnet characteristics and features:

In order for a network simulator to be effective in all kinds of projects and ventures related to network research and development, it requires four main characteristics:[27]

* Flexibility: the capability of simulating different network protocols / applications under a wide range of operating conditions.
* Robustness: the capacity to provide powerful users with modeling, simulation and data analysis equipment.
* Ease of use: users need to find the learning curve flexible and easily attainable.
* Clarity: the simplicity of identifying occurring modeling problems and simulation errors.

OPNET is acclaimed by network professionals because it has all the aforementioned characteristics. It can be adapted to go to almost every network protocol creators need, network service providers, also like network equipment manufacturers.

OPNET is an assortment of software that has been designed with an extensive set of features. These features make it to be highly comprehensive software. Some of these features are as follows:[10]

* + The capacity to study and examine using built- in graphing tools.
  + Object-oriented models. Which means a model can be used as a reference or as a logical extension of object notions.
  + Opnet allows for comparisons and concurrent simulations between multiple scenarios.
  + Opnet offers the option to import traffic models into the software.
  + Network models of a hierarchal nature. Meaning the model can be ingrained inside layers.

## Opnet Applications:

* + - * **Management of application performance:** Opnet includes ACE Analyst to analyze network apps, ACE Live to analyze network at a real-time basis as well as observe the experience of end-users, etc.
      * **Planning:** Such as IT/SP Guru Network Planner used for planning networks for companies and SPs (service providers).
      * **Engineering:** IP/SP Guru Network Planner can also be used for engineering, alongside SP Guru Transport Planner.
      * **Operations:** For operations, Opnet offers SP Sentinel for network review, safety and policy-compliance strategies for SPs (service providers).
      * **Development and research:** This encompasses Opnet Modeler, Modeler Wireless

Suite…[30]

## Opnet editors:

**Project editor:** The Project Editor is the main region to create a network simulation. From this editor, you can build a network model using the standard library templates, choose the network statistics, run a simulation and view the results.



## Figure III.2 project editor interface [26]



**Figure III.3 Project editor icons [26]**

OPNET version 14.5 has a list of icons. Each one offers a specific functionality, as listed below:

1-Open object palette 2-Fail selected objects

3-Recover selected objects 4-Go to parent subnet

5-Zoom to rectangle 6-Zoom to previous

7-Import topology from ACE 8-Import topology from device configurations

9-Import topology from VNE server 10-Open traffic center

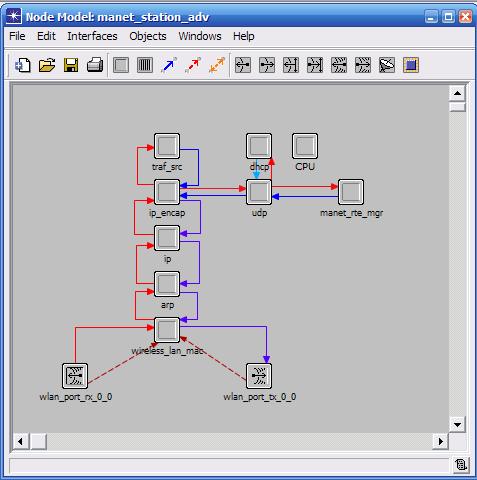
1. Configure/run Netdoctor
2. Generate network difference report
3. Configure/run flow analysis
4. Configure/run survivability analysis
5. Configure/run discrete event simulation (DES)
6. Configure/run design action
7. Configure/run automation tasks 18-Web – Open report server home 19-View results
8. Hide/show graph panels
9. Generate network inventory summary
10. Launch network to assess readiness of network to IPV6
11. Migrate existing network to IPV6

**Node editor:** The Node Editor allows you to define the behavior of each network object. The behavior is defined by using different modules, each of which models some internal aspect of node behavior such as data creation, data storage, and so on. The modules are connected by packet streams or statistical wires. A network object is composed of typically multiple modules that define its behavior.

The modules that we use to build the network can vary between process, queue, or transceivers.[25]

Using the process model, one can entirely program the processes. Additionally, queues have the ability to manage data packets and buffer them.

There are also two kinds of interfaces between modules: Packet streams or Statistic wires.



## Figure III.3 node editor interface

**Process editor:** Allows you to create process templates, which control the underlying functionality of the node templates created in the Node Editor. The operations performed in each state or for a transition are described in C embedded or C ++ code blocks.

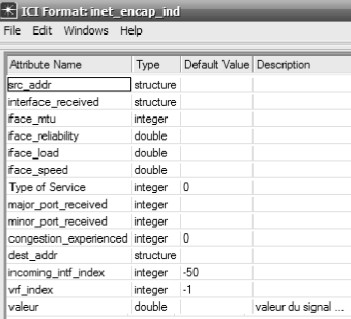
The process model is constructed of diagrams for state transitions, C codes in the form of blocks, OPNET Kernel Procedures, variables of states and finally variables that are temporary in nature. [25]

Processes can not only respond to interrupts, but they can also generate child processes in a dynamic manner. They can also have one of two states, forced (green) and unforced (red).



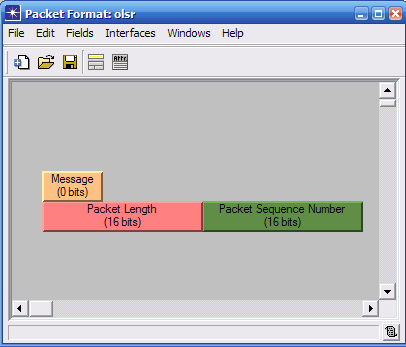
## Figure III.4 process editor interface[25]

**ICI editor:** The Interface Control Information editor allows for the definition of the internal structure of interface control information. ICIs are used to formalize the interconnection between interruption-based processes. ICIs can also be used to deliver supplementary information in regards to creating interruptions. The type of attributes can be selected out of three option: Integer, Structure or Double, and one can set a default value.[29]



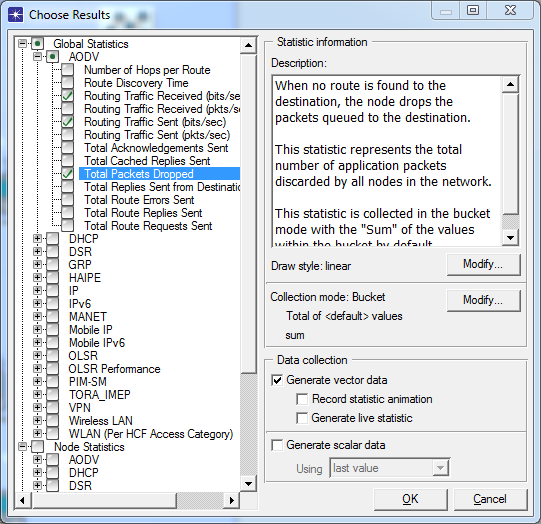
## Figure III.5 ICI editor interface [29]

**Packet format editor:** The packet format editor gives the ability to define the internal structure of a packet in the form of a list of fields to complete. A packet format contains one or many fields, represented in the editor as colored rectangular boxes. The boxes’ dimensions can vary and are equivalent to the number of specified bits that represent the fields’ dimensions.[30]



## Figure III.6 Packet format editor interface [30]

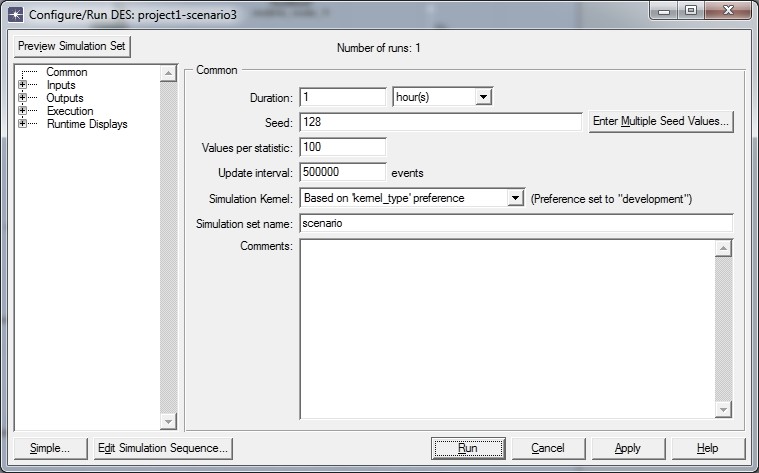
* + 1. **Running a Simulation:** After having defined all the models of the network system, we can validate it by simulation in order to study the performance and behavior of the system. Generally, there are three steps for simulation execution and the collection of information:
       1. **Statistic Collection:** The developed models must always decide which information should be extracted from the simulation. These can take various forms including visual animations, time-dependent series (vector), and parameterized (scalar) ratios.



## Figure III.5 choose individual statics

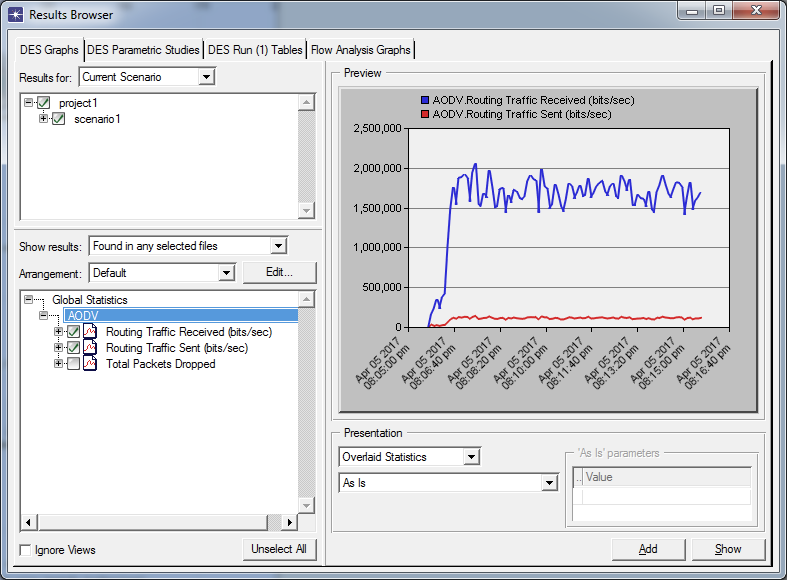
* + - 1. **Configuring Simulations:** OPNET provides a number of options for performing simulations, including internal and external execution, and the ability to configure attributes that affect the behavior of the simulation.

Scenarios automatically provide a default duration and random number seed for simulations. Users can set simulation attributes by choosing “Configure Simulation” from the Simulation menu, or by clicking on the “running man” icon.



## Figure III.6 configuring run simulation

* + - 1. **View results:** After having configured the simulation we can view the results in the forms of graphs that allows us to compare results of different scenario even from different projects.



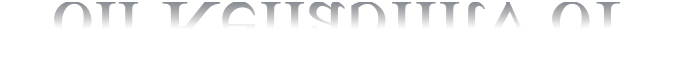
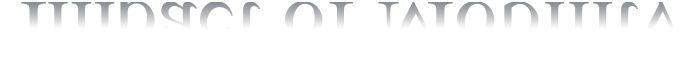
## Figure III.7 view results

These results can vary in their form. They can be scalars (a list parametric input reliant values) that are not planned in accordance to time, animations that represent the flow of packets or the movement of nodes, or vectors (Pairs of time-value that are listed).

# III.7 Conclusion:

Opnet is a very powerful tool used in many disciplines of network design and troubleshooting. With this tool, the network parameters and their effects on the network performance can be thoroughly comprehended and deduced.

OPNET Modeler was chosen as a simulation environment because it is one of the leading environments for network modeling and simulation. It supports a large number of built-in industry standard network protocols, devices, and applications. In addition to that, its programming library helps researchers to easily modify the network elements and measure their performance in the simulation environment. OPNET also provides rich data analysis features.



# introduction:

A Mobile Ad hoc Network (MANET) is a set of mobile nodes that communicate with each other without any pre-existing infrastructure.

In MANET, due to dynamic topology, mobile nodes move freely any time, towards any direction in the network. Mobility is an important characteristic in MANET that plays a crucial role in determining the reliability of the network this is because of the high mobility of nodes that can cause frequent changes in network topology, leading to less reliable routes and more link breakages, as a consequence, increasing the reinitiating of the route discovery process, resulting in more packets dropped and increasing the delay.

# Mobility in ad hoc networks:

## definition:

The main advantage of MANET is the ability to maintain communication while being mobile. However, this mobility advantage in MANETs also presents a constraint for the management of the network. Frequent and dynamic changes in the network topology are caused by node mobility. Roads can be created and disappear very often, and suddenly, for varying periods of time. These displacements naturally have an impact on the network. They can change the network topology and the behavior of the wireless communication channel.

For proper network management, these changes must be taken into account as soon as possible by the routing protocol in order to ensure a correct view of the topology of the nodes. The reactivity of the routing protocol to these changes has a direct impact on the reliability of routes. The routing protocol uses the routing metrics to select the best route. In the case of sudden or rapid mobility, there will be a delay between the values of the actual metrics and those taken into account by the routing protocol. This implies packet dropped because the routing tables are not updated sufficiently in time, with the correct metric values.

Mobility is a random phenomenon that affects the quality of wireless communications. The modeling of wireless communications is very complex in general. In addition to mobility, it is necessary to model the physical system, on the one hand, and also to model the interactions between the protocols of the different layers during the communication, on the other hand.

For example, in an urban environment, the mobility of terminals depends only on the mobility of the people who transport them. Mobility impacts performance of routing protocol.

## mobility models:

* **Random waypoint:** In this model, nodes are distributed randomly in the network and move randomly towards any direction with random speed, which is uniformly distributed between in Min and Max Speed. Also the destination is selected randomly where nodes move in the network they have a pause time (they stopped for a period of time) before choosing another destination.
* **Static vector:** The static vector mobility model and no targeted destination fall under the category of random mobility models. It saves mobility state for nodes and also in the current mobility state allow only partial changes, only natural moves are reproduced. This model generates a random vector mobility with no targeted destination. This model has many advantages like easily implemented, simplification for node’s position updates and also provides mobility prediction occasion.

# Related works:

## Performance evaluation of routing protocols in MANETs under FTP traffic applications:

Mohammad Amin Roshanasan, Jia Uddin, and Md. Monirul Islam wrote a paper to assess the OLSR and AODV routing protocols with OPNET simulator under the medium load traffic size in FTP protocol. The Random Waypoint mobility model is used. They chose to examine the average throughput and average network load in different number of nodes, file sizes, and node speeds.

They used OPNET version 17, and in all the scenarios established, all mobile devices used IPV4. Three types of different scenarios were made based on the number of nodes, different file (data) sizes, using performance metrics as average throughput and average end-to-end delay for AODV and OLSR.

They used four different packet sizes (512, 1024, 2048, and 4096 bytes), a fixed MANET size of 1km X 1km, a different number of nodes (20, 40, 60, 80, 100), varying speeds (50,30,5).

They studied the impact of file size under different speed and the impact of density on performance of AODV and OLSR.

In their conclusion, they found that proactive protocols perform better with average throughput and average end-to-end delay. OLSR protocol performs well as it displays lower end-to-end delay and higher throughput. The OLSR delay has very slight changes when the numbers of nodes grows.[37]

## Impact of mobility models on routing protocols for various traffic classes in mobile ad hoc networks:

In his thesis, Hayder Majid Abdulhameed Alash led a comparative analysis of numerous routing algorithms with a few prevalent mobility models while varying traffic patterns.

He has made simulation models that include two mobility models (Random Waypoint, and Group), all the classes of routing protocols in MANETs (Hybrid, Proactive, and Reactive), all with three types of traffic patterns (Variable bit rate, random, constant bit rate). As a simulation software, the author used QualNet.

Their simulation parameters included a 1.5 Km X 1.5 Km area with 50 nodes, a simulation period of 1000 seconds, a node speed that ranges from 0m/s to 10m/s, routing protocols of all classes (FSR, OLSR, ZRP, AODV, and DYMO) and a data rate of 2Mbps.

His results are as follow: Throughput:

It was noted that throughput elevates when the number of nodes rises. Thus, and it will increase performance. It will also elevate when the speed increases, but it is contingent on the type of routing and what is the optimal maximum speed selected in the random waypoint mobility model. AODV was found to have the best performance of the routing protocols in this regard in random traffic and constant bit rate traffic, while OLSR was the best in variable bit rate traffic.

Average end-to-end delay:

AODV was found to outperform all other protocols in each traffic class in the random mobility model. But in group mobility model, ZRP outperforms the others.

Average Jitter:

Again, AODV shows the best results in the random waypoint mobility model, while in group mobility model, ZRP performs better than the rest. [38]

## The impact of mobility models on the performance of mobile Ad Hoc network routing protocol:

Megat Farez Azril Bin Zuhairi, M and Zafar, Mohammad Haseeb and Harle David have selected in their paper, three distinct mobility models, each with its own nodes movement behavior. They also presented a new measurement technique called probability of route connectivity, which they have used to measure the success rate of routes created by a routing protocol. They ran extensive simulations to compare each mobility model. They have evaluated the performance of Ad Hoc on demand distance vector (AODV) in a network made of various intensity of unidirectional links against three mobility models.

The mobility models they have studied and experimented on are:

The Gauss Markov Mobility Model: a proposed model for the purpose of overcoming the faults of Random Waypoint Model. Essentially, nodes determine their next vector to the next location based on past speed and direction. Due to its complexity of computing node movement, it is seldom used in simulations.

The Reference Point Group Mobility Model: The best way to describe how this model functions is to compare it to the movement of a group of rescue teams in disasters (Earthquakes…etc.) where each individual node is influenced in its movement by the group’s movement pattern.

The Manhattan Mobility Model: nodes in this model can only move based on a number of predetermined paths that are organized in a block pattern. It is primarily used to simulate mobile nodes in city street environments.

The observed results focusing on the number of unidirectional links generated by AODV clarify that at a higher speed, the chance of unidirectional links occurrences is higher. Also, at higher speed, routes become more unsteady and possibly break, causing unidirectional links. Averagely speaking, the Gauss Markov mobility model produces more unidirectional links compared with the other two models studied in this paper. [39]

## Analyze the Impact of Mobility on Performance of Routing Protocols in MANETs Using OPNET Modeler:

Narinder Pal, Renu Dhir have assessed in their paper the performance of ad hoc routing protocols AODV, OLSR and GRP, under Random Way Point and Vector Mobility models by considering three parameters: delay, network load, and throughput.

They have used two scenarios in OPNET 14.5, one with 75 nodes and the other with 150 nodes, on a static 3.5 X 3.5 Km area. HTTP and FTP were chosen as traffic types. The 802.11 data rate was of 11Mbps, and all of this was simulated in a time of 300 seconds.

Concerning throughput, they have concluded that OLSR performs better than the other two protocols in the simulations, and that it’s better paired with vector mobility model than the random waypoint model. OLSR also has an advantage when it comes to route breaking, since it always has updated topology information available, whereas AODV and GRP need to discover the route in order to transfer information.

Delay wise, OLSR outclasses AODV and GRP again, whatever the network size in question is. This is due to the proactive nature of OLSR allowing it to process intermediate nodes quicker. It was also observed that random waypoint mobility had a higher delay than the other model used because the nodes in the network move unpredictably. [40]

## The Impact of Mobility on the Performance of AODV and DSR Using NCTUns 6.0 Simulator:

G. Vijaya Kumar’s paper tackles the theme of mobility and its influence on the performance of routing protocols AODV and DSR. Multiple scenarios of mobility are used to investigate and conclude which of the aforementioned protocols outperforms which, and under what conditions. He evaluated the performance of AODV and DSR using three metrics packet delivery ratio, delay and number of control packets.

The open source, Linux-based network simulator NCTUns 6.0 was used to carry, set and investigate the comparative simulations.

The simulation setup accounts for 50 nodes in the topology, five pairs of which are used for communication, all on a terrain of 1km X 1km surface. The initial nodal positions are random, using Random Waypoint mobility model. A maximum speed of 10m/s was set, and a simulation time of 100 seconds was configured. Packet size was decided to be 1400 bytes, with a CBR traffic model.

The results of the author’s simulations show that DSR outperforms AODV in high mobility.

In conclusion, all mobility rates, the DSR is better than AODV in terms of throughput, network delay and routing overhead. [41]

## Optimized and Reliable AODV for MANET:

Srinivas Sethi proposed an Optimized Reliable Ad hoc On-demand Distance Vector (ORAODV) scheme that allows quick implementation of dynamic link conditions, low processing and low network utilization in ad hoc networks. By implementing Blocking Expanding Ring Search (Blocking-ERS) and retransmission of data packet in ORAODV, it provides satisfactory performance in term of packet delivery ratio (PDR), normalizing routing load (NRL) and delay for different network density in term of number of node, various mobility rates.

Their proposed scheme (ORAODV) is designed for optimal route discovery and reliability of packet delivery. Every broadcast is delivered with a hop number which is a serial number designating the sequence of the nodes in a route from the source. When a node desires to know a route to a destination node, it inundates the network with a RREQ message.

Intermediate nodes receive the RREQ message and examine their routing table. If the route information is not available for the destination node, the intermediate nodes rebroadcast the RREQ with an incremental hop number. In this manner, the nodes with the same hop number from the source node form a circle or searching ring which expands as the process of discovery of routes continues.

They use a new control packet caled “stop instruction” which is used to regulate the flooding,

and a hop number to decrease the energy consumption during route discovery.

For their simulations, they have used NS-2 simulator in the Linux operating system to compare between the proposed protocol and AODV in terms of performance. CBR was picked as a traffic model, each node has a queue of 50 packets that await transmission. A 1km on 1km area is used as a simulation stage, while the number of nodes ranges from 50 to 300, increasing every time by 50. Mobility rate is changed between 1, 5, 10, 15, and 20 m/s.

The performance metrics that were chosen for this simulation are Packet Delivery Ratio (PDR), Normalized Routing Load (NRL), and end-to-end delay.

The results show that ORAODV performs better than AODV in terms of end to end delay, especially in a higher nodal density. Normalized Routing Load was also found to be better for ORAODV than for AODV, especially for a higher number of nodes. ORAODV was found to perform better in different mobility rates. Packet Delivery Ratio was found to be better in ORAODV with a fixed mobility rate. [43]

## Mobility aware routing protocol in Ad-hoc network:

Suman Halder, Partha Pratim Meta and Sukla Banerjee proposed a new mobility-aware routing protocol based the AODV routing protocol called: MA-AODV (Mobility

Aware Ad-hoc On Demand Distance Vector) in order to try and improve the treatment of high mobility factor in ad-hoc networks. MA-AODV protocol perform episodic quantification of nodes’ mobility in order to establish steadier paths between source and destination pairs, hence, avoiding the frequent link ruptures associated with using unstable paths that contain high mobile nodes.

In their network model, they assume that all nodes are GPS enable and that they are connected to each other with bidirectional antenna, the range of each one being equal.

They also assume that all communication is symmetric between the nodes.

Since their objective is to minimize the problems that arise from node mobility in AODV, especially link breakage, their proposed methodology operates in such a way that an optimal static path is chosen instead of the shortest path. They slightly modified the HELLO message of AODV which is broadcasted by each node among its neighbors to maintain its routing table, by adding three position parameters with the HELLO message of AODV: Altitude, Longitude, and Height. Each node will copy these parameters in its respective routing table. Based on these parameter each node can calculate the distance and velocity between it and their neighbors, in order to send the reply packet to the neighbor that converging to it.

They have simulated their proposed algorithm using JAVA Applet. The simulation procedure concurrently executed two algorithms, one being the Mobility Aware Routing Protocol (MARP) which they have proposed, and the other being the Non Mobility Aware Routing Protocol (NMARP). The simulation was done in an 800 x 800 Applet window for different number of nodes, and of different velocity.

They have compared data routing paths from source to destination between the two protocols, and the results show that MARP’s frequency of link breakage is much lower than that of NMARP’s. It also showed that their proposed MARP always selected static paths compared to other protocols. The rate of broadcasting messages (HELLO, RREQ…Etc.) was found to be lower in MARP, as well as the energy loss for sending these messages. MARP was also shown to be suitable for sending large data where constant connection is required between the source and the destination. [44]

## A new metric for adaptive routing in mobile Ad hoc networks:

Rahem ABRI ZANGABAD proposed a new metric called hop change metric to present the changes in the network topology due to mobility. Hop change metric characterizes the variations in the number of hops in the routing table. It is believed that the variation in the hop count is a good representative of mobility. The high number of change in the hop count can be a sign of high mobility. This metric is implemented in two popular and main routing

protocols. The AODV protocol and the DSDV protocol using the LA-AODV (Lightweight Adaptive) approach that selects routes with low degree of mobility and the LA-DSDV approach that helps determine a threshold value based on the aforementioned metric in order to decide the full update time dynamically and cost effectively.

The author experimented on simulations using NS-2. Packet delivery ratio, network overhead, drop rate and end to end delay are the parameters from which data is analyzed. The simulation layout was done in a 1km on 1km area, with 100 nodes whose speeds range from 0 to 20m/s, using CBR packet traffic mode and random waypoint mobility model.

The results of the author’s simulations show that LA-AODV had an enhanced performance in all performance metrics. There are significant improvement compared to the original AODV from point of packet delivery ratio, end to end delay, network overhead and dropping rate.

The change range between ADOV and LA-AODV from the point of network throughput is almost 5%. Therefore, it was concluded that LA-AODV is far superior to the original AODV. It was also concluded that the hop change metric represented the topology changes due to mobility well and it could be used for determining the full update time adaptively.

The results also support the belief that the author’s approach based on hop change metric improves the packet delivery ratio and the packet drop rate with a practical increase in the overhead and the end-to-end delay. [45]

# impact of mobility on reliability of AODV:

* + 1. **presentation:** our contribution aims to study the impact of mobility on reliability of AODV. Based on specific parameters as end-to-end delay, total packets dropped and throughput. we studied the reliability of AODV which can be affected by node’s speed and we tested max speed that can be supported by AODV also the impact of mobility in large network.

From the previous works, Narinder Pal and Renu Dhir studied the impact of two mobility models (vector and random) on AODV, OLSR and GRP using three performance metrics throughput, load and delay

The authors, R.Aoudjit, M.Lalam,M.Belkadi ,measure the impact of speed on AODV by two metrics control packets and packets reception fraction.

Also, Narinder Pal and Renu Dhir presented a comparative study of the impact of two mobility models (mobility vector and random) on AODV, GRP, OLSR.

But our contribution is a complete study on the impact of mobility on AODV. We prove the impact of mobility by different speed from a low speed to high speed to test the limit of AODV that doesn’t tested before. We also determine the impact of speed in large networks.

## different tests or investigations:

* + - * **investigation of speed :**in this part we studied the impact of speed on reliability of AODV that can be measured by mentioned parameters where we used low speed as human speed, medium as vehicular speed and high speed that represents a helicopter speed that can be used in rescue mission or as ambulance used by civil protection.
      * **Investigation of maximum speed:** we tested the maximum speed that can be supported by AODV. This high speed can be used in military.
      * **Investigation of density: we** tested the impact of speed in network with different numbers of nodes, to prove the impact of mobility in large networks.
      * **Investigation of mobility model:** we tested the impact of the two mobility models static vector and random waypoint on the reliability of AODV.

## modifying AODV parameters:

AODV routing protocol has many parameters that affect its reliability. We choose the most important one, hello message.

Due to mobility, links could break and route become unavailable.

In order to detect this failure, AODV uses the "HELLO " control messages to verify the connectivity of the routes. A node determines the connectivity of a route by periodically listening to the "HELLO " messages transmitted by its neighbors. In case of default AODV, if for a period of time, three HELLO messages are not received consecutively, the node considers that the link to this neighbor is broken.

Our modification is augment number of loss hello message to 20, which means link could break and AODV cannot detect it.

This test aims to prove the importance of route maintain especially in dynamic topology that changes frequently with high speed.

# AODV with new speed metric:

Based on our study we prove that AODV is affected by mobility, that’s why we proposed an approach to enhance the reliability of AODV.

While AODV selects the route with the minimum hop count, our approach aims to select the best route to destination based on speed of nodes to increase the reliability of AODV.

It means selecting the most stable route where nodes have a low degree of mobility and more stable using speed nodes as new metric.

The new metric will be defined like that : AODV\_cost = node\_speed.

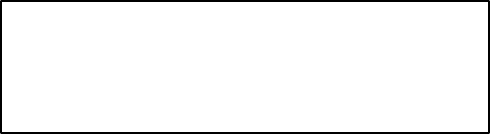
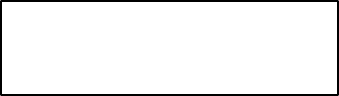
AODV routing protocol will select the route that has less speed instead of min number of hops.

This metric to be functioning, we changed the following :

* + - Route request mechanism
      * Add the AODV\_cost to RREQ packet.
      * When an intermediate node receive an RREQ with the same sequence number and lower cost, forward it.
    - Route reply mechanism
      * The destination node send RREP with the cumulative cost.
      * The source node will forward its data packets to destination using the route with min speed (AODV\_cost).

We present our proposition as below:

Begin



No

Existing route ?

Yes

* The source node initiate a route

discovery process

* Creation of RREQ with

AODV\_cost

Source node forward

packets to destination

Intermediate node recieve the RREQ

No lesser

Existing route ? Compare SN ?

Yes

Sends a RREP to the source

Equal or

higher

Compare the cost ?

Dropped the RREQ

lesser

Dropped the RREQ



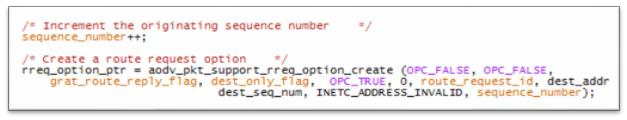
Equal or

higher

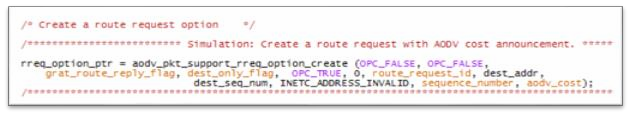
* Cumule the AODV\_cost.
* update the routing table entry.
* broadcast RREQ to it’neighbors.

## Figure IV.1 proposition route discovery

## source code modification



**Figure IV.2 RREQ of default AODV**



**Figure IV.3 RREQ of modified AODV**

* + 1. **Parameters used in the network**

In order to prove the impact of mobility on reliability of AODV, the following parameters are considered:

* + - * **Throughput:** is defined as the ratio of the total data packets reaches to a specific receiver node from a sender node in the time which it takes.

Throughput is represented in bytes or bits per second (byte/sec or bit/sec). Throughput is the average rate of a perfect message delivery in a specific transmission link in simulated network that affects, if there are many topology changes in the network, unreliable communication between nodes and limited bandwidth available. A high throughput means a high reliability.

* + - * **Delay:** Represents the end to end delay which is the time that a data packet needs to reach a destination. This is the time when the source node starts transmitting the first packet to its receiver. Transmission delay is the time taken to transmit all the packets on the link while propagation delay is the time taken to transmit first bit to reach the destination. Processing delay is the time taken by all processes between source and destination. When using reactive routing protocols it needs to calculate a delay for route discovery. In a MANET, the delay is higher than wireless network because of the limited signal power, mobility, established routes, and failed connections because of dynamic topology. End-to-end delay is used to measure the impact of different mobility models and various traffics on different routing protocols.
      * **Total packets dropped:** When the source node doesn’t find a route is to the destination, the node drops the packets queued in buffer to the destination.

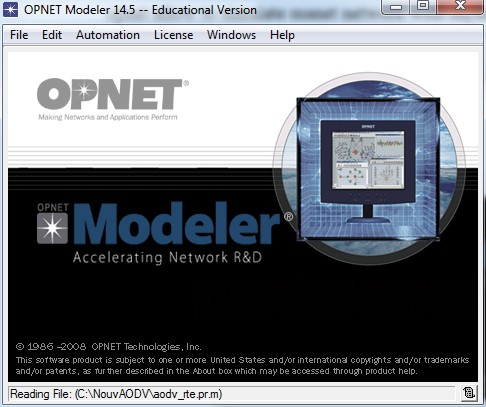
This statistic represents the total number of application packets discarded by all nodes in the network.

# implementation of our contribution:

## chosen simulator:

Opnet simulator allow modeling and simulation of communication networks, due to its library models (routers, switches, mobile nodes, server….).

Opnet allow to simulate MANET network with different protocol and parameters.



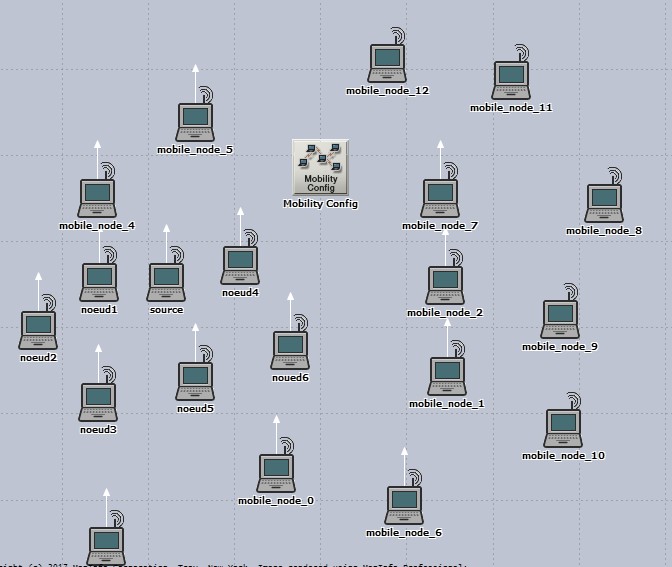
## Figure IV.4 Opnet modeler 14.5

* + 1. **network simulation:**

To simulate the protocol AODV under different speeds and mobility models. The simulation by opnet go through many steps:

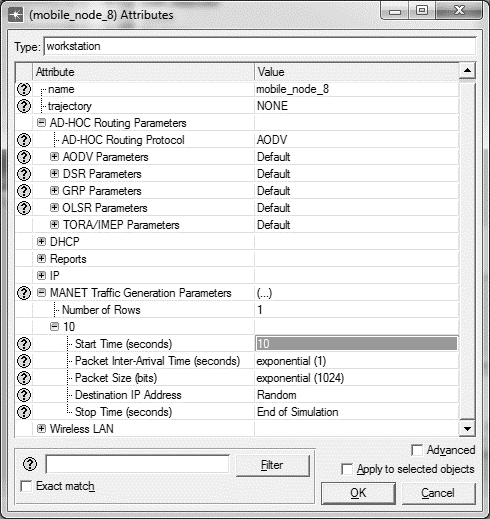
* + - * **First step :** it consist to simulate ad hoc network like that :

Execute opnet => file => new project => initiate the topology => insert network components (mobile node, mobility config…).



## Figure IV.5 simulation network

* + - * **Second step :** after the insertion of the components passing to the configuration network step (choosing AODV protocol, determine speed of nodes and mobility model)

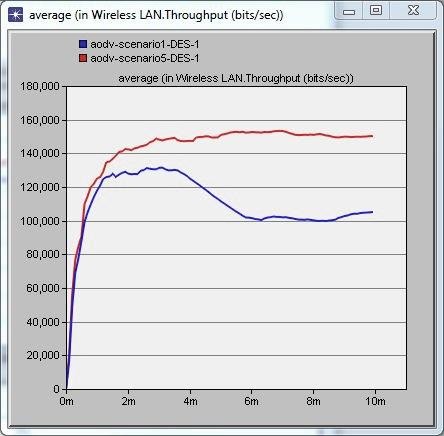


## Figure IV.6 AODV configuration

* + - * **Third step: execution** of simulation (run). In this step we can specific Simulation time

## Forth step: view results

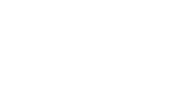
Show graphs of simulation results and compare the results of different scenarios.



## Figure V.7 Throughput

# IV.7 Conclusion:

The principal goal of this chapter is to describe our contribution that consist to study the impact of mobility on reliability of AODV with different tests, using Opnet simulator, and present our approach to enhance AODV by changing the route selection metric from hop count to node speed. In next chapter we will simulate many scenarios with different parameters and analyze the results.



* 1. **Introduction:**

In order to test the reliability of protocol in a network, it is not always possible to access the necessary infrastructures because of their high costs. As we said before, ad hoc networks are networks which include several mobile units that move in any territory and whose only means of communication is the use of radio interfaces.

Indeed, it would be very expensive, if not impossible, to set up a network for testing certain criteria. To remedy this problem, it was necessary to resort to simulation which provides the user with a fairly complete experimentation environment.

In this chapter, we presented our tests and results to show the impact of mobility on reliability of AODV. We studied the effect of speed, maximum speed and mobility model on the reliability of this protocol that can be measured by end to end delay, throughput and total packets dropped. Also, we presented the results of comparison between the default AODV and our modified AODV.

# Simulation Setup:

We experimented AODV routing protocol with different speed. We created many scenarios to prove the impact of mobility on reliability of AODV. The simulation parameters are included in Table 1.

|  |  |
| --- | --- |
| **Simulator Opnet 14.5** | |
| **Dimension** | 5X5 km |
| **Number of nodes** | 20,25,30,35 ,40,45,50 |
| **Routing protocol** | AODV |
| **Technology WLAN** | 802.11g |
| **Simulation time** | 10 minutes |

## Table V.1: Network Parameters

|  |  |  |
| --- | --- | --- |
| **Scenario** | **Speed (m/s)** | **Mobility model** |
| 01 | Uniform(0,5) | Random waypoint |

* 1. **investigation of speed:**

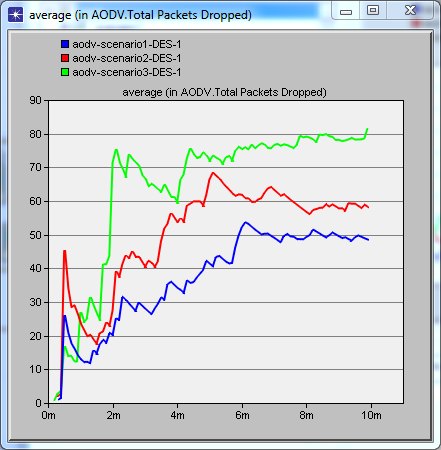
|  |  |  |
| --- | --- | --- |
| 02 | Uniform(0,30) | Random waypoint |
| 03 | Uniform(0,100) | Random waypoint |

**Table V.2 simulation scenarios**

* + 1. **total packets dropped:**

In figures 1 and 2, the results obtained for total packets dropped are shown. This parameter increase with speed, it means when speed increases, total packets dropped increase.

As a result, total packets dropped increase because of high mobility of nodes where the packets cannot reach the destination and get dropped.



## Figure V.1: total packets dropped

## for 20 nodes

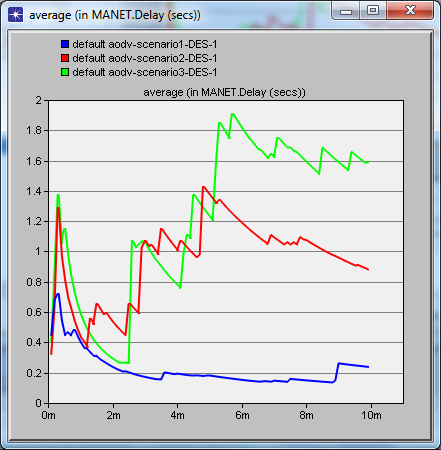
65

## Figure V.2: total packets dropped for 25 nodes

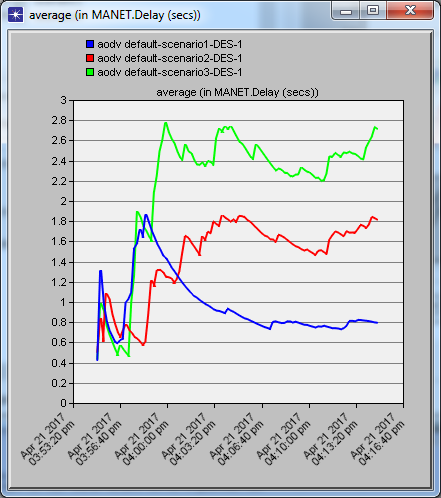
* + 1. **End to End delay:**

As shown in figure 3 and 4 the delay increase when speed increase.

As we mentioned before the delay is the time taken by packet from its creation to reach the destination.

Because of mobility of nodes, source node doesn’t find a valid route to the destination so the data packets are stored in buffer until find a valid route, as consequence the delay increase.

## Figure V.3: delay for 20 nodes

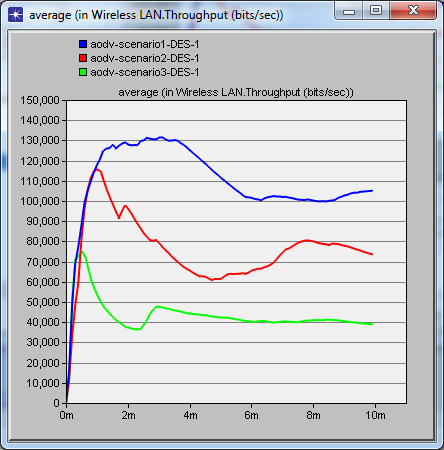


**Figure V.4: delay for 25 nodes**

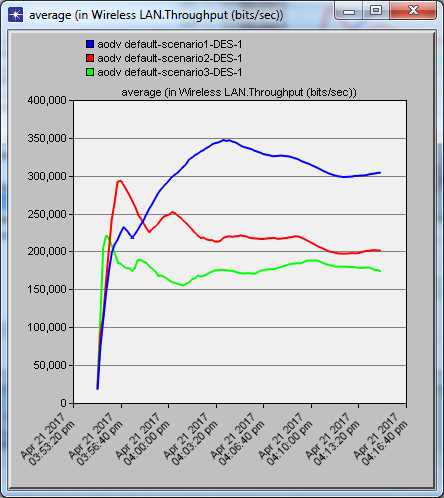
* + 1. **Throughput:**

As shown in figure 5 and 6 throughput decrease when speed increase.

When nodes move with high speed, the topology changes frequently. Due to unavailable routes, packets are dropped, as result number of packets that reach the destination successfully decrease that means throughput decrease.



## Figure V.5: throughput for 20 nodes



**Figure V.6: throughput for 25 nodes**

* + 1. **conclusion of investigation of speed:**

AODV provides good results in low speed, but in high speed routes will change frequently so source node doesn’t find a valid route to destination so packets are dropped, as consequence packets that reach the destination successfully decrease, it means decrease the throughput.

AODV as a reactive protocol initiate a route discovery process which increase delay because packets are buffering until find a valid route.

As result, high speed degrade the reliability of AODV, it means has a negative influence on reliability.

# investigation of density:

## total packets dropped:

As shown in figure 7 total packets dropped per nodes increases when number of nodes increases but still the graph of high speed has more dropped packets.

The speed of nodes has more effect in large networks where there is more traffic circulate in the network which increase the total packets dropped.

As result, in network with 40 nodes number of packets dropped per nodes increase with 100%.



Total packets dropped versus number of nodes

9

8

7

6

5

4

3

2

1

0

20

25

30

35

number of nodes

40

45

50

5 m/s

30 m/s

100 m/s

packet dropped per nodes

## Figure V.7 total packets dropped versus number of nodes

## End to End delay:

As shown in figure 8, delay increases when number of nodes increases but still the graph of high speed spend more delay.

The speed of nodes has more effect in large networks where the number of hops per second increase which increase the delay and because of mobility of nodes ,routes changed so until find a valid route data packets are buffering which increase the delay.



End to End Delay versus number of nodes

12

10

8

6

4

2

0

20

25

30

35

Number of node

40

45

50

5m/s

30 m/s

100 m/s

End to End Delay

Figure V.8 End to End Delay versus number of nodes

## Throughput:

As shown in figure 9, throughput increases when number of nodes increases but still the graph of low speed has more throughput.

In network with 50 nodes the throughput decrease by 60% in comparison between speed of 5m/s and 100m/s.



Throughput versus number of nodes

30000

25000

20000

15000

10000

5000

0

20

25

30

35

Number of nodes

40

45

50

5 m/s

30 m/s

100 m/s

Throughput per nodes

## Figure V.9 Throughput versus number of nodes

## conclusion of investigation of density:

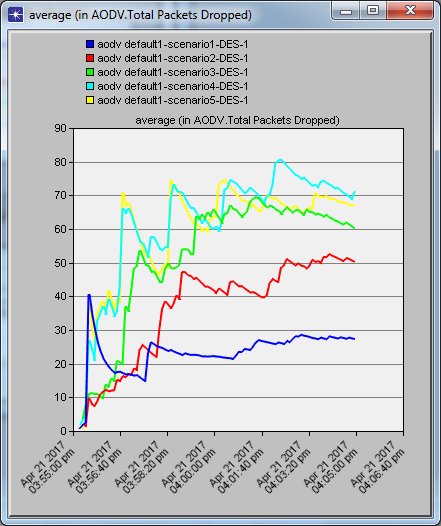
The speed of nodes has more effect in large networks where the number of hops per second increase which increase the throughput and because of mobility of nodes, routes changed so the source node initiate a route discovery process to find a valid route and packets are dropped which decrease the throughput and increase the total packets dropped in high speed.

As result, the speed of nodes is so influential in large networks.

|  |  |  |
| --- | --- | --- |
| **scenario Speed (m/s) Mobility model** | | |
| **01** | Uniform(0,5) | Random waypoint |
| **02** | Uniform(0,30) | Random waypoint |
| **03** | Uniform(0,100) | Random waypoint |
| **04** | Uniform(0,500) | Random waypoint |
| **05** | Uniform(0,600) | Random waypoint |

## Table V. 3 simulation scenarios

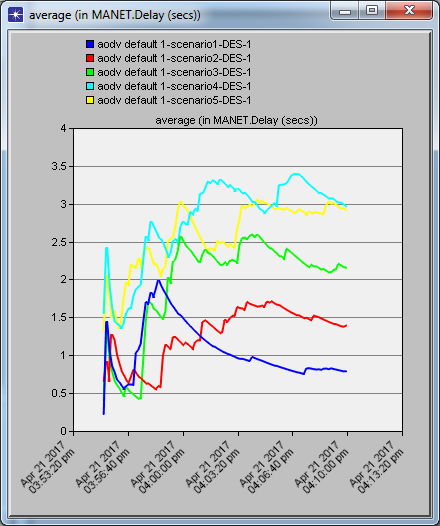
* 1. **investigation of maximum speed:**
     1. **total packets dropped:**

Figure 10 shows that graph of scenario 5 with 600m/s converge to graph of scenario 4 with 500m/s.

## Figure V.10 Total packets dropped with different speed

* + 1. **End to End delay:**

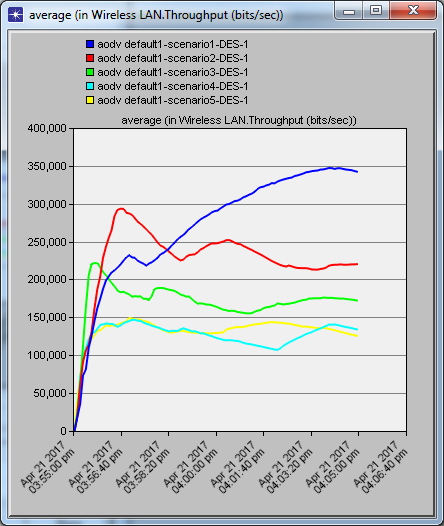
Figure shows that graph of scenario 5 with 600m/s converge to graph of scenario 4 with 500m/s.



## Figure V.11 End to End delay with different speed

* + 1. **Throughput:**

The same as dropped packets and delay, figure shows that graph of scenario 5 with 600m/s converge to graph of scenario 4 with 500m/s.



## Figure V.12 Throughput with different speed

* + 1. **conclusion of maximum speed:**

Maximum speed that AODV routing protocol can support is 500 m/s.

In case of higher than that speed, results converge to the same ones as 500 m/s.

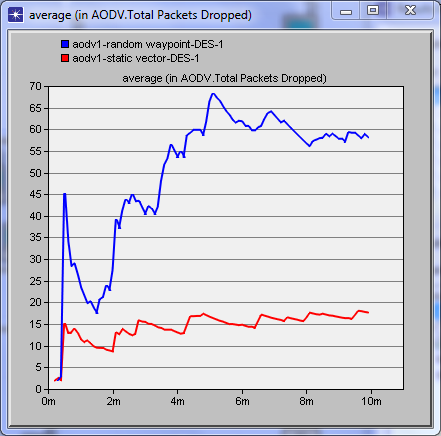
# investigation of mobility models:

|  |  |  |  |
| --- | --- | --- | --- |
| **scenario** | **Speed (m/s)** | **Mobility model** | |
| **01** | Uniform(0,30) | Random | waypoint |
| **02** | Uniform(0,30) | Static | vector |

## Table V.4 simulation scenarios under mobility models

* + 1. **total packets dropped:**

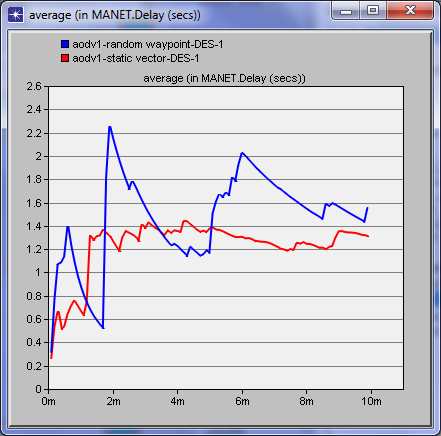
Figure 13 shows that scenario with static vector model on 10 min of simulation time it reaches 19 as max value but scenario of random waypoint reaches 79 packets dropped.



## Figure V.13 Total packets dropped under different mobility models

* + 1. **End to End delay:**

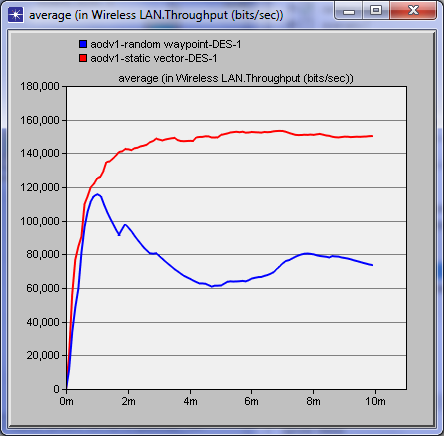
Figure 14 shows that AODV under static vector provides good delay which reaches 1.4 sec as max value but random waypoint increase to 2.2 sec and increase to 1.6 sec.



## Figure V.14 End to end delay under different mobility models

* + 1. **Throughput :**

Figure 15 shows that AODV under static vector provides good throughput which reaches 150,000 bit/sec as max value but random waypoint decrease to 40,000 bit/sec and increase to 50,000 bit/sec.



## Figure V.15 Throughput under different mobility models

* + 1. **conclusion of mobility models:**

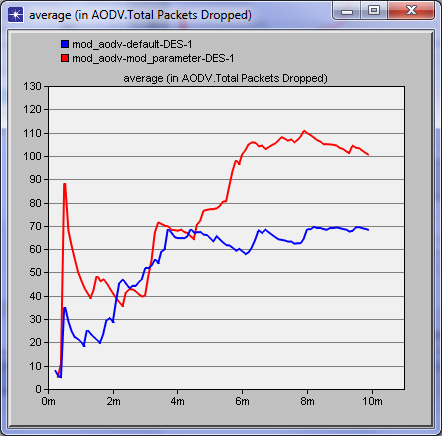
AODV under static vector provides good results. On the other hand AODV under random waypoint doesn’t provide good results because nodes move randomly and routes change frequently which increase packets dropped and as consequence decrease throughput(number of packets that reach the destination successfully) and increase delay because of unavailable route.

# modifying AODV parameter:

We created two scenarios, default AODV and the second one, we augment the number of lost Hello message.

## total packets dropped:

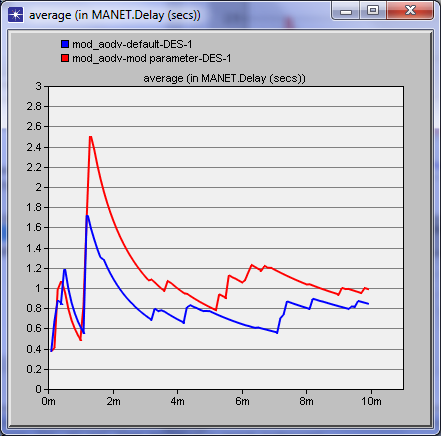
The AODV with high number of lost Hello message has more dropped packets.it increase to reach 80 dropped packets.



## Figure V.16 Total packets dropped comparison

* + 1. **End to End delay:**

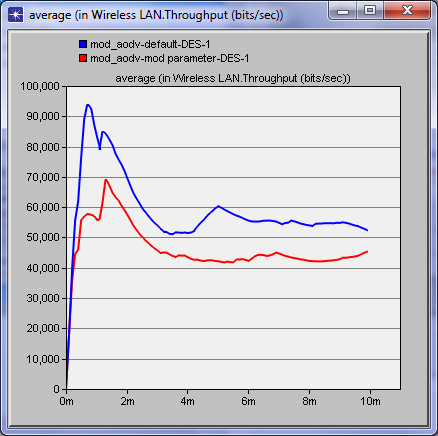
The figure shows that the default AODV has the shortest delay. While the AODV with high number of lost hello message has a long delay.



## Figure V.17 delay comparison

* + 1. **Throughput :**

The figure shows that throughput of modified AODV decrease, because of absence of maintenance.



## Figure V.18 Throughput comparison

* + 1. **conclusion:**

From the previous results we have proved that the absence of route maintenance in mobility network degrade the reliability of AODV, that is cleared by decreasing of throughout and increasing of delay and packets dropped.

In absence of route maintenance links break, it means route become unavailable but it still exist in routing table as active route, which increase the dropped packets.

Due to dynamic topology, routes change frequently and links break, but Hello message is used to verify the connectivity and realize stability in network.

# AODV with new speed metric

We realized two tests, the first one is to compare the reliability of default and modified AODV under speed of 10m/s. The second one is under speed of 100m/s.

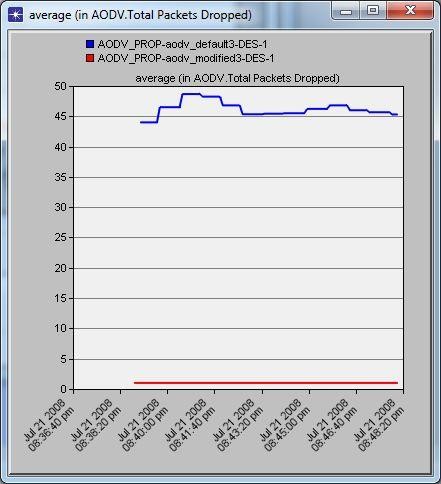
## First Test:

|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Speed (m/s)** | **Mobility model** | |
| **01** | Uniform(0,10) | Random | waypoint |

**Table V.5 First test**

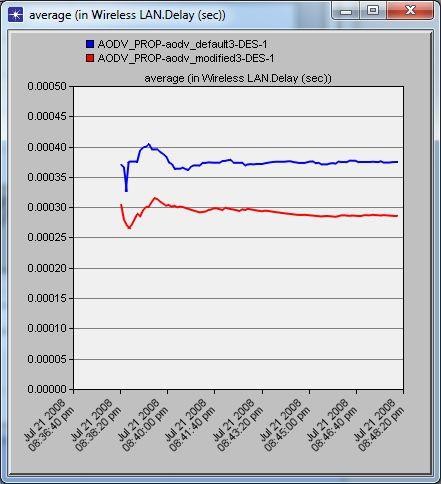
* + - 1. **Total packets dropped:**

As it shown the modified AODV based on speed metric has less packets dropped that equals to one but default AODV dropped the average of 45 packets.



## Figure V.19 total packets dropped comparison between default and modified AODV

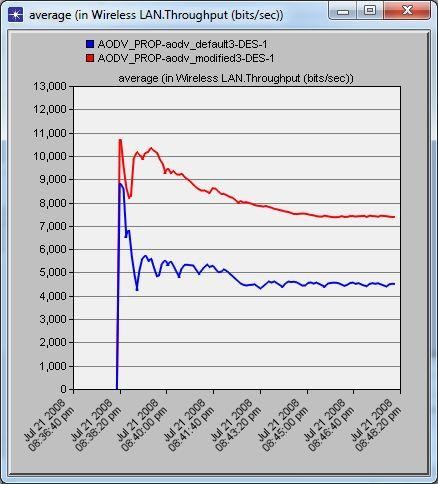
* + - 1. **end to end delay:**

As it shown the modified AODV based on speed metric has the shortest delay that equals to 0, 0003 but default AODV takes the average of 0, 00037 m/s.

## Figure V.20 delay comparison between default and modified AODV

* + - 1. **Throughput:**

As it shown the modified AODV based on speed metric has the best throughput that equals to 7500 bits/s but default AODV has the average of 4500 bits/s.



## Figure V.21 Throughput comparison between default and modified AODV

* + 1. **Second Test :**

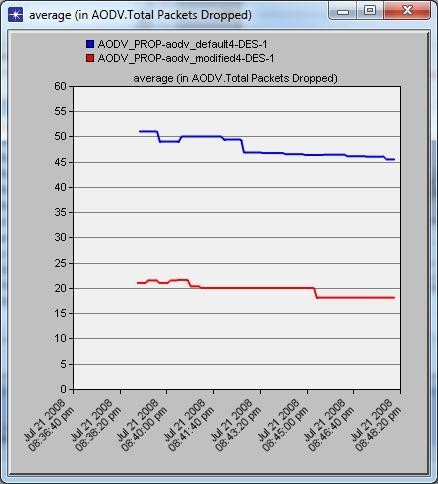
|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Speed (m/s)** | **Mobility model** | |
| **02** | Uniform(0,100) | Random | waypoint |

**Table V.6 Second Test**

* + - 1. **Total packets dropped:**

As it shown, because of high speed the dropped packets of the two scenarios increase, but it still that modified AODV has less dropped packets.

The default has the average of 45 but the other has 20.

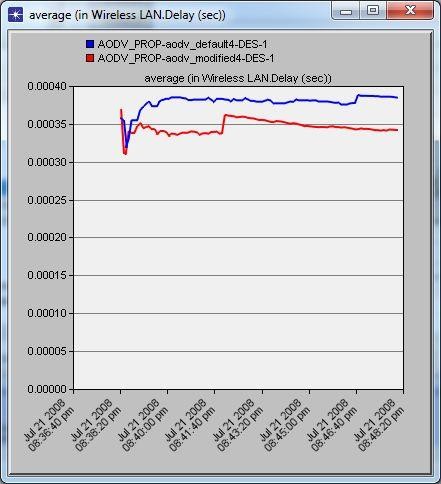


## Figure V.22 total packets dropped comparison between default and modified AODV

## End to End delay:

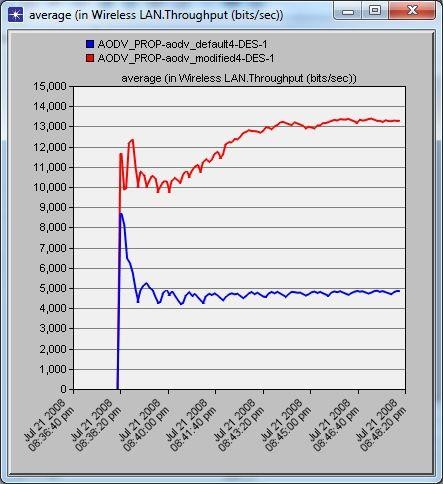
As it is shown, because of high speed the delay of the two scenarios increase, but it still that modified AODV has less delay.

The default has the average of 0,00039sec but the other has 0, 00035 sec.



## Figure V.23 delay comparison between default and modified AODV

* + - 1. **Throughput:**

As it is shown, the throughput of the modified AODV is higher than the default. Even with high speed modified AODV provides results better than The default.

## Figure V.24 Throughput comparison between default and modified AODV

# V.8.3 conclusion of the two tests:

The improved or the modified AODV provides good results.

Due to mobility, nodes which move quickly lose their reliability and increase links break. As a consequence routes become unavailable and that guides AODV to initiate a route discovery process to find a valid route where packets are dropped which decrease the throughput and increase the total packets dropped. Also the delay increase because packets are buffering until find a valid route.

As a conclusion selecting route less mobile and more stable improve the reliability of AODV compared to default AODV. For example, when speed ranges from 0 to 100m/s throughput has been increased by more than 2 times (260%).

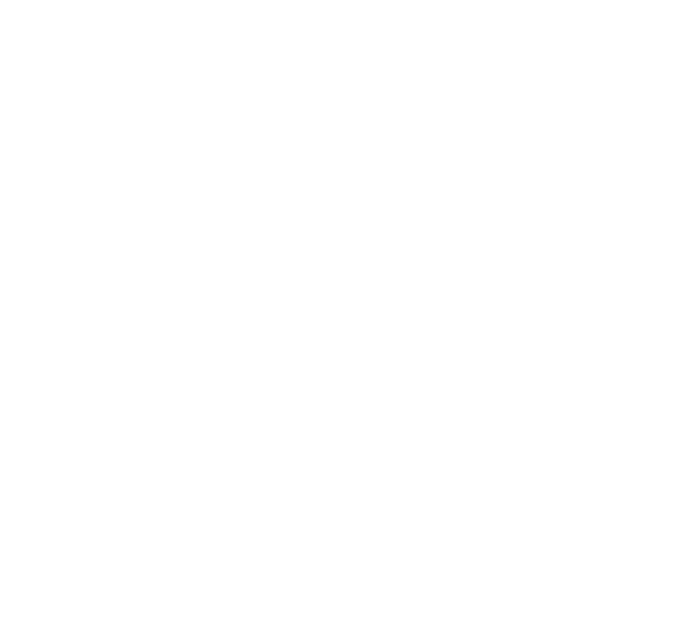
# V.9 conclusion:

From the results of different investigation, mobility is crucial characteristic that has a negative influence on reliability of AODV.

The reliability of AODV is affected in high speed where we measured it with some parameters as throughput, delay and total packets dropped.

We can also conclude that the speed of nodes is so influential in networks. On the other hand, we prefer static vector as mobility model.

From the results obtained in comparisons between our modified AODV and the default AODV, we conclude that the new proposed metric (node speed) of new route selection gives better network reliability results than the default metric (number of hops).



# General conclusion:

Recently, mobile networks have become increasingly needed in more and more areas of life as technological progression is fast and unstopping, and it requires those who use networks and devices to keep up.

Due to their offering end-users and hosts the ability to move freely while still being part of an existing network and communicate, Ad hoc networks are accumulating more attention, more focus and more recognition with the passage of each year.

But despite their advantages, routing remains a steadfast issue as different protocols aim for the ideal performance and reliability of the network.

It is in that context that our work has been set to focus on the AODV protocol, researched and found to be better performing compared to its counterparts in ad hoc networks. This project proves the impact of mobility on the reliability of AODV by testing it’s reliability under different speed and different mobility models,we also tested the impact of speed in network with high density.And get the result that the mobility has a negatif influence

on reliability of AODV.

In the second part of our contribution we proposed a modified AODV protocol with new speed metric.In purpose to improve the reliability of AODV this modified protocol select the route less mobile and more stable.The results indicates that our approach enhance the reliability of AODV.

## Future works and perspectives:

In regards to future works and perspectives, here are some ideas of projects:

 Study the impact of mobility on the stability and performance of the network using other performance metrics.

 Make an extensive research on other MANET protocols (OLSR…etc.) by testing the

impact of mobility on their reliability.

 Alter initial AODV parameters (default parameters) and study the impact of mobility of these new parameters on the stability and performance of the network.

 Propose another metric or combine between many existing metrics to reduce the impact of mobility on the stability and performance of the network.

 …etc.

# References

[1] Nicolas Daujeard and Julien Carsique and Rachid ladjadj and Akim Lallemand, " le routage dans les réseaux mobiles ad hoc", ed ingénieur , pp 5,9,12-27,2003.

[2] Mr Boukhechem Nadhir, "routage dans les réseaux mobiles ad hoc par une approche a base d'agents",mémoire de magister, Université Mentouri de Constantine,2008,pp 4-20.

[3]S. BASAGNI, M. CONTI, S. GIORDANO and I. STOJMENOVIC, " MOBILE AD HOC

NETWORKING", 1st ed. Piscataway, New Jersey: IEEE Press, pp. 262-270, 2017.

[4] BERRABAH Abdelkrim,SAIDI Hassiba, "Balancement de charges dans les réseaux Ad Hoc",mémoire de master, université abou bakr belkaid– Tlemcen,pp13-16,2013.

[5] Krishna Gorantala, "Routing Protocols in Mobile Ad-hoc Networks", Master’s Thesis in

Computing Science, Umea University,SWEDEN,pp 7,13-19, June 2006.

[34] J.Hoebeke, I.Moerman, B.Dhoedt and P.Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Ghent University – IMEC vzw,Sint Pietersnieuwstraat Ghent,Belgium,pp 61,2004.

[7] Muhammad Arshad Ali and Yasir Sarwar, "Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions", Master Thesis, School of Computing Blekinge Institute of Technology, Sweden,pp 17-22, March 2011.

[8] Fatima AMEZA, "Les technologies sans fil: Le routage dans les réseaux ad hoc (OLSR et AODV) ",mémoire master, Université de Bejaia,pp 20-27, 2007.

[9] Amadou Baba BAGAYOKO, "Politiques de Robustesse en réseaux ad hoc",Thése Doctorat,Université Toulouse,pp 11,17,2012.

[10] Agustin Zaballos, Alex Vallejo, Guiomar Corral, Jaume Abella, "AdHoc routing performance study using OPNET Modeler", Barcelona (Spain,pp 1,2),2004.

[11] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR) ", Project Hipercom,pp 4,8,October 2003.

[12] Kamil CHEBIRA, "Etude et analyse de la stabilité des protocoles de routage dans les réseaux ad-hoc", Mémoire présenté en vue de l’obtention du Diplôme de Magister en Informatique, Université Hadj Lakhdar BATNA,pp 33-37, 2007.

[13] Sabrine NAIMI, "Gestion de la mobilité dans les réseaux Ad Hoc par anticipation des métriques de routage ", Thèse de doctorat,pp 7-15, juillet 2015.

[14] Raja S R , Dr.K.Alagarsamy, "Analysis QOS Parameters for MANETs Routing Protocols Using AODV And DSR", International Journal of Innovative Research in Science, Engineering and Technology,Volume 3, Special Issue 3,pp 1016,1017, March 2014.

[15] Tayeb lemlouma, "Le Routage dans les Réseaux Mobiles Ad Hoc",master thesis, Université des Sciences et de la Technologie Houari Boumèdiene,pp 24,39, 2000.

[16] Ignacy Gawe˛dzki, "algorithmes distribués pour la sécurité et la qualité de service dans les réseaux ad hoc mobiles",thèse de doctorat de l’université paris-sud 11 spécialité informatique, pp 23\_30,29, septembre 2008.

[17] Kanishka Raheja , Sunil Kr Maakar, "A Survey on Different Hybrid Routing Protocols of MANET", International Journal of Computer Science and Information Technologies, Vol. 5, pp 512-514,2014.

[18] Omar Cheikhrouhou, "Sécurité des réseaux ad hoc", mémoire ingéniorat, l’Ecole Nationale d’Ingénieurs de Sfax,pp 26-32, juillet 2005.

[19]D. Dr. Kamaljit I. Lakhtaria, "Analyzing Reactive Routing Protocols in Mobile Ad Hoc Networks", Int. J. Advanced Networking and Applications, vol. 3, no. 6, pp. 1418,1419, 2012.

[20] M. Singh and S. Kumar, "A Survey: Ad-hoc on Demand Distance Vector (AODV) Protocol", International Journal of Computer Applications, vol. 161, no. 1, pp. 38-44, 2017.

[21] C. Perkins, "Ad hoc On-Demand Distance Vector (AODV) Routing", E. Belding-Royer University of California, Santa Barbara,2013,pp 7-11.

[22] C. Edward Perkins and R. Samir, "Ad hoc On-Demand Distance Vector (AODV) Routing", International Journal of Emerging Technology and Advanced Engineering, vol. 4, no. 3, pp. 12-16, 2000.

[23] P. Thakral, "An Overview of AODV Routing Protocol", International Journal of Software and Web Sciences, vol. 7, no. 1, p. 49, 2014.

[24] Sheng Liu, Yang Yang and Weixing Wang, Research of AODV Routing Protocol for Ad Hoc Networks, AASRI Conference on Parallel and Distributed Computing and Systems, Elsevier,2013,p 23-26.

[25] Xinjie Chang, Network Simulations With Opnet, Proceedings of Simulation Conference, Network Technology Research Center School of IEEE,1999,pp 307-309.

[26] Z. Lu and H. Yang, "Unlocking the power of OPNET modeler", 1st ed. Cambridge: Cambridge University Press, 2012,pp 24-39.

[27] Andrew Kim, OPnet Tutorial,pp 12-15, March 7, 2003.

[28] T. Srikanth and D. Narsimha, "Simulation-based approach to performance study of routing protocols in MANETs and ad-hoc Networks", IJCSNS International Journal of Computer Science and Network Security, vol. 11, no. 9, pp. 111,112, September 2011.

[29] A. Maria, "Introduction to Modeling and Simulation", Proceedings of the 1997 Winter Simulation Conference, pp 7,8, 1997

[30] Yannick GRENZINGER and Loic Jaquemet, “Project Opnet”,Opnet Technology,Inc,

pp 2-4,2004.

[31] v. ravi, "SDP Implementation in MANET using OPNET Modeler 17.5", Final project Report,SFU, 2014,pp .

[32] F. Faret. e. P. Nonnon, "Une approche intégrée de la modélisation scientifique assistée

par l’ordinateur," Aster, 2006.

[33] G. B. e. L. Lerman, "Modélisation et Simulation", pp 12-14, 2015.

[34] H. Bossel, "Modeling and Simulation", Library of Congress Cataloging- in-Publication Data,2004,pp 24-26.

[35] M.humayun kabir, I.syful, MD.Javed, H.sazzad, Detail Comparison of Network Simulators, International Journal of Scientific & Engineering Research, Volume 5, Issue 10,

October-2014,pp 204-206

[36] K.Atta ur Rehman, Sardar M.B and O.Mazliza, A Performance Comparison of Network Simulators for Wireless Networks, University of Malaya, LP 50603, Kuala Lumpur, Malaysia,2012,pp 2-3.

[37] J. U. M. M. I. Mohammad Amin Roshanasan, "Performance Evaluation of Routing Protocols in MANETs Under FTP Traffic Applications," International Journal of Electronics & Communication Technology, vol. 3, no. 4, 2012.

[38] H. M. A. Alash, IMPACT OF MOBILITY MODELS ON ROUTING PROTOCOLS FOR VARIOUS TRAFFIC CLASSES IN MOBILE AD HOC NETWORKS, M.S., Kent

State University, 2016.

[39] M. a. Z. M. H. H. D. Megat Farez Azril Bin Zuhairi, "The impact of mobility models on the performance of mobile Ad Hoc network routing protocol.," The Institution of Electronics and Telecommunication Engineers, vol. 29, no. 5, 2012.

[40] R. D. Narinder Pal, "Analyze the Impact of Mobility on Performance of Routing Protocols in MANET Using OPNET Modeller," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 6, 2013.

[41] G. V. Kumar, "The Impact of Mobility on the Performance of AODV and DSR Using NCTUns 6.0 Simulator," International Journal of Computer Science And Technology, vol. 4, no. 2, 2013.

[42] R. PUROHIT, "Analysis Of The Impact Of Mobility On Aodv," Suresh Gyan Vihar University Journal of Engineering & Technology, vol. 1, no. 1, 2015.

[43] S. Sethi, "Optimized and Reliable AODV for MANET," International Journal of Computer Applications, 2010.

[44] P. P. M. a. S. B. Suman Halder, "Mobility Aware Routing Protocol Ad-Hoc Network," Natarajan Meghanathan, et al., pp. 30, 2012.

[45] R. A. ZANGABAD, " A New Metric For Adaptive Routing In Mobile Ad Hoc Networks", Master thesis, Institute of Sciences of Hacettepe University,pp 25-29, 2014.