INTERNATIONAL
HELLENIC
UNIVERSITY

Theoretical analysis of a wireless mesh network

Kareklas Thomas

SID: 3301110006

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

OCTOBER 2012

THESSALONIKI – GREECE

INTERNATIONAL
HELLENIC
UNIVERSITY

Theoretical analysis of a wireless mesh network

Kareklas Thomas

SID: 3301110006

Supervisor: Prof. Costas Tzaras

Supervising Committee Member: Assoc. Prof. George Koutitas

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

OCTOBER 2012

THESSALONIKI – GREECE

Abstract

This dissertation was written as a part of the MSc in ICT Systems at the International Hellenic University. The purpose of this dissertation is to explore the issues of mesh networking protocols and techniques for Advanced Metering Infrastructure (AMI). A mesh network is the configuration of peer wireless access nodes that allow for continuous connections to a network infrastructure, including reconfiguration around blocked paths, by “hoping” from node to node. By AMI we mean systems that measure, collect and analyze energy usage information from advanced metering devices through various communication media.

More specifically the entire paper is divided in 2 axes:

a) Theoretical: it contains two chapters where there is a report of 3 topologies (Star topology, Tree topology, Mesh topology) trying to identify in which way each one of them can be applied in home or neighborhood area network. The perspective is which one could support more efficiently AMI. Moreover, there is a detailed description of the protocols used by the above topologies as well as the protocols used by commodity smart meters.

b) Practical: we used Opnet Modeler to simulate and investigate which is the most optimal combination of the theoretical part. Specifically, there are many cases available where we tested many different configurations to explore how a network could be more efficient and tolerant.

In order for this dissertation to be accomplished, the contribution of Dr Tzaras, Dr Koutitas and the academic staff of International Hellenic University was very important and useful.

Furthermore, I would like to thank especially my family, Peter, Efi and Christine for their support. Special thanks to Ntek, Geros, Vasi, Vagg, Kriti, Chryssi, George Em, Nikos Red, Peter, Helen K, Kathrine, John Pap, Semina, Apostolos.

Thomas Kareklas

Date 29/10/2012

Contents

1 Introduction

1.1 AMI

Advanced Metering Infrastructure (AMI) is the existing infrastructure so that devices that consume energy such as electricity, water or gas to be controlled and managed remotely in totally innovative and different way that we used to know until now. Actually, it is the infrastructure that connects devices with the utilities that provide the consumed energy distributing this energy across the different parts that AMI consists of. This is happening with the meters that are implemented which are the brain of the overall infrastructure. They share information about the energy consumption to the users, to the utility but also to the competitive retail providers. AMI operates in a bidirectional way since allows the necessary energy to traverse along the infrastructure in order to be consumed by the devices but also returns back the required metrics that the utilities demand from the devices.

The motivation for the AMI to be implemented was to reach the goal of reducing human intervention in energy cost optimization. The main characteristics of the AMI must be:

- Redundancy of nodes is required so that every consumer can be included.
- Bidirectional communication among the components of AMI
- The security principal (Confidentiality, Integrity and Availability) should be provided by the system in order for the meter data to securely traverse the system and to be properly delivered to the utility.

Regarding to the last characteristic AMI must provide service management monitoring of the meters to ensure the security of the system but also to be able to control manage more elements such as tampering, rate delivery and many other useful information for energy management efficiency.

The AMI could consist of four components:

1. Utility company
2. Concentrator (Data Collector)

3. Smart Meter (SM)

4. Home or Office

and has six paths enabling interfacing between the components.

AMI is based on a sensor system (computer based) which connects the buildings (the energy consumed by residents) to the utilities (companies that provide, manage and pricing this energy). Technically AMI could be defined as the processes and functions that are used in order for these energy management services to exist in both utility companies and consumers. As a consequence, all parties included in this infrastructure can decide appropriately about reducing costs, covering the energy demand and posing throughputs dealing with the periods of high demand and assuring the normal energy distribution along the network.

As far as the Utility company and Concentrator are concerned, their major role is to provide the necessary capabilities to reassure the security of the most important metering systems that already exist.

The concentrator includes two interfaces:

- NAN interface, which enables the communication with the meter
- WAN interface, which enables the communication with the company

The concentrator may act as an intermediary between the meter and the utility or as storage location loaded embedded with a capable buffer memory.

On behalf of utility the WAN collector, through the WAN interface, gathers the needed information or sends alerts-alarms signals that are generated by the event manager. The Master Data Management Service (MDMS) has the role of billing and system operation, while the portal module provides consumers with the display of the recorded meter data and bills.

The Smart Meter (SM) measures the energy consumption and includes the necessary cards to share and receive information with the Concentrator and the Home (or Building). Furthermore, it contains Remote Disconnection Function which delivers and receives control messages giving the opportunity the service to be connected or disconnected remotely. The bidirectional sharing of data (information about power management, energy recording etc) among the devices with the individual meters and the Collector defines the NAN.

The Home (or Building) uses the Home Gateway to implement the communication with the meter and have the Controllers so that consumers can control the energy that they consume.

Sub-meters could also be used to reinforce the usage information by residents' devices. In the AMI architecture the sub-meters could be supplementary to the main meters that are used in order to unburden the computational needs and to allow more accurate recordings.

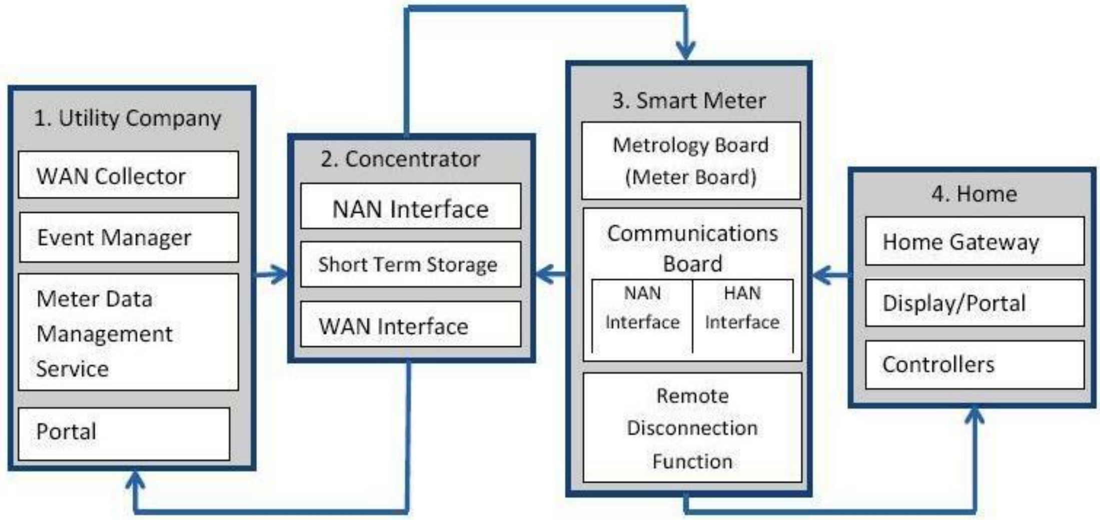


Figure1: AMI components [1]

Finally, AMI is a quite demanding infrastructure that consists of many processes, functions, devices and data that must be managed properly and securely. It can maintain three or even more different types of networks (WAN, NAN, HAN).

1.2 Topologies

There are three topologies that we examine in this dissertation that can support these networks; Star topology, tree topology and mesh topology. In a star topology the communication is taking place among a central node (coordinator) and the rest nodes which are controlled and exchange information immediately with the central node and afterwards among them. In a tree topology there is a hierarchy where the first level is considered to be the root (a central node) and each layer is connected to the next layer constructing a tree. In a mesh network there is more flexibility since it is not necessary a central node to coordinates overall the topology and that is the major reason that gives many advantages to this topology. Each node is responsible of forwarding the packets which means that every node is an autonomous router. However, it is possible for a mesh network to have such an operation with a coordinator if it is necessary.

When the infrastructure is established and the appropriate topology is selected for a network, we have to decide what protocol will be implemented in order for the network to be served in the most efficient way for the occasion. For this purpose we analyze two types of protocols in the dissertation. Initially, there is a report of routing protocols where we analyze proactive and reactive protocols. Specifically, there is a detailed description of the OSPF, OSLR, DSDV, AODV in order to explain how the routing can be done and which protocol could be implemented for different cases that we will examine in the next chapters.

1.3 RF Mesh protocols

An extensive report and explanation of various RF mesh protocols is available in chapter 3. The reported protocols are CSMA, CSMA/CA, ZigBee and Z-Wave. These protocols are implemented in different devices in order to be used in daily basis. Their purpose is to facilitate the users (either they are used in houses or in companies) to manage easily and more efficiently the energy amounts that they consume.

1.4 Simulations

The fourth chapter deals with the experimental procedure. There are several simulations available that have been run, so that we are able to identify how specific parameters are able to affect a network's (HAN or NAN) operation. Opnet Modeler is the application that was used to build and run our simulations.

Opnet stands for Optimized Engineering Tools, a graduate project for a course in networking at MIT, networking software that became the company OPNET Technologies in 1986. The software, is a network simulation tool including features and toolsets and a packet format that defines protocols, a node model for specifying network component interface, a process model for abstraction of behavior of a particular network component, a project window for defining the topology of the network and various linkages and a simulation window that is able to capture and show the results of network simulation having compiled the simulation firstly.

In this dissertation we used this technology in order to built and plan our networks and mainly to simulate them getting all the results that we needed in order to extract safe results.

We used two protocols 802.15.4 and 802.11 to test Home Area and Neighborhood Area Networks respectively. We configured our networks in a variety of parameters in order to testify the tolerance, efficiency and operation of the networks.

Finally, having estimated the results we took from the simulations we cite our conclusions and our perspective for the future work that should be made.

2 Network topologies for Advanced Metering Infrastructure

HOME AREA NETWORK

A Home Area Network (HAN) consists of smart meters, smart interconnected devices with sensors and actuators and home energy management system which deals with the consumed energy in a household. Home networks may be used as residential broadband for personal computers, video games, tablets and many other entertainment devices. Moreover, home networks may interoperate with external networks such as Internet form Internet Service Providers or Telecommunications Companies. The most important issue in a HAN is to manage its devices interconnected exchanging data and information among them demanding minimum human intervention. To accomplish that the selection of the physical medium and as well as the communication protocols are a major issue. In many cases we do not have the sufficient coverage by these issues due to various factors such as environmental factors or building's bad architecture, consequently we can use **star**, **tree** or **mesh** topology to overwhelm these difficulties.

More specifically, every device that joins a Home Area Network is enabled to have services that would not have otherwise, operating lonely. It becomes part of a network within which can communicate with other devices exchanging data with them and being managed and control in a total different way by its user. Establishing a Home Area Network the user has the facility to control the included appliances, the home's condition and the energy consumption of the overall network with the same manner either inside the home or remotely. A similar management can be done as far as the utilities are concerned since they receive data concerning to the services they provide reassuring for the proper function, security and billing of them.

The difficult task of such a network is the maintenance of the heterogeneous devices and their technologies. In the next chapter there is a detailed report of the existing protocols that have been invented to accomplish that.

NEIGHBORHOOD AREA NETWORK

In a Neighborhood Area Network multiple HANs are connected distributing information concerning the energy consumption and the control and use of different home appliances. NAN and HAN communication takes place through the network technologies and protocols that are used by both of these area networks. Actually NAN has a role of an access network allowing HANs to communicate with other HANs and WAN. NANs provide ubiquity meaning that every device location communicates with many other devices that are located thousands of square miles away. However, there are some requirements that there have to be fulfilled such as power efficiency, reliability, low cost, communication efficiency, low latency, security etc. Both of these area networks are of great importance for an Advanced Metering Infrastructure as they facilitate the utilities to have access to the consumers' personal area as far as the meters are concerned and also facilitate the consumers themselves to have an unknown, until now, flexibility as for the automation of their devices' use. We will discuss how the **star**, **tree** and **mesh** topology meet the needed requirements to support NAN's operation.

2.1 Star topology

In the star topology there is a main node acting as a central clustering device or as an access point or as a concentrator serving the rest nodes of the network. The communication takes place in a holistic way meaning that every node entering the network that wishes to contact with the rest nodes of the network has to send its entire data to the concentrator which is responsible to deliver the sender's data to the receiver. A device has usually the role either of the start point or of the end point in the communications networks. The concentrator can be the node that begins or complete or routes the data transferred through the network and therefore it is the master node that controls completely the network topology. Every single device that is considered to be part of the network in every topology has a unique 64-bit address that can be used for instant communication with the rest devices inside the PAN. What is more, every single device of the network could have more short address of 16 bits, as well. Since the concentrator demands high load of energy consumption to execute its duties in the star topology the 802.15.4 standard suggests the concentrator to be supplied permanently with energy whereas the rest nodes of the network to use most likely batteries for their operation[18],[19].

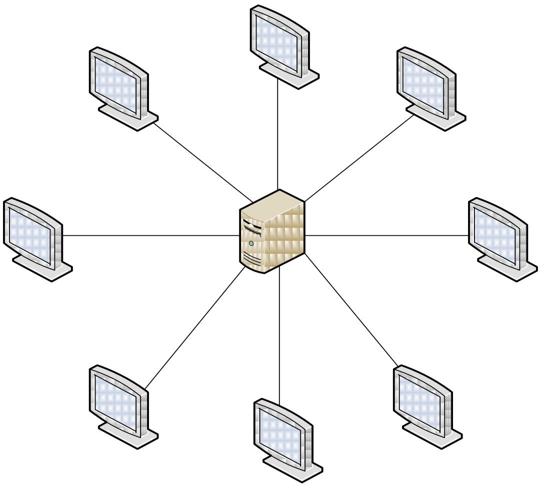


Figure 2.1: Star Topology

Advantages [2]:

- Because every device contacts to the coordinator individually if one device (node) or cable fails, it brings down only that specific node without affecting the entire network. This is a major benefit since it reveals that using this topology a fault tolerant network is established and flexible enough for the damage to be troubleshooted. Furthermore, this topology provides great scalability to the network since any device-node that wants to be part of the network has nothing to do but contact to the central node.
- Transmissions are virtually collision-free.
- The management of the network is quite easy. The fact that all the devices communicate with a central device (coordinator) that could be server, hub switch minimizes the needed cost for entire the network. This central device should be mostly protected. Moreover, this central device facilitates the administration of the network, too.
- A variety of network media can be used to attach to the centralized devices, making it easier to merge legacy and new networks.
- Data transfer speeds of 4, 16, 100, 1000 Mbps are now specified in IEEE 802.5.

Disadvantages [2]:

- A failure of the central device (coordinator), such as a server or a hub, would cause a general failure in the network since no device could have communication.
- In a wired network environment, cable costs can be higher than they would be in other topologies because of the length of the cabling used to connect nodes to a central device.
- Throughput speed is given up for collision-free transmissions.

ADVANTAGES	DISADVANTAGES
Coordinator	Coordinator
Transmissions collision-free	High cost for wired topology
Easily managed network	Limited throughput speed
Easier to merge legacy and new networks	

Table 2.1: Advantages and disadvantages of Star topology

2.2 Tree topology

Tree topology, known and as hierarchical network, has many common functions with star and bus topology. Actually it could be characterized as combination of them. As it is shown in the figure 2.2 this topology looks like an inverse tree. There is one top level central node (root) which is connected to other nodes of lower levels in the hierarchy and these nodes are connected to other nodes of lower levels than their level and so on and so forth following this hierarchical pattern. In this way the branches and the trunk of the tree are created. There have to be at least three hierarchical levels and two branches otherwise it has no difference with a star topology network.

The structure of this topology allows us to have multiple servers on the network and to branch out the network variously. Actually, in this topology links and nodes are arranged to distinct hierarchies enabling in that way easier control and troubleshooting. This serves completely the colleges, universities and schools as each one can work independently in its own network but also to be part of the bigger network.

When the root node transmits signals to the network, they are received simultaneously by all the nodes increasing by this way the network's efficiency. Furthermore, the nodes do not act as generators or repeaters for the signal to be transmitted. To avoid this, the nodes exchange data among them not having the root as an intermediary in their communication as it happens in the star topology. Finally, the Tree topology can be extended to function and to size since there are not limitations about how wide the topology could be. Specifically, it is feasible an additional central node to be added having two different trees being interconnected within the same network [17].

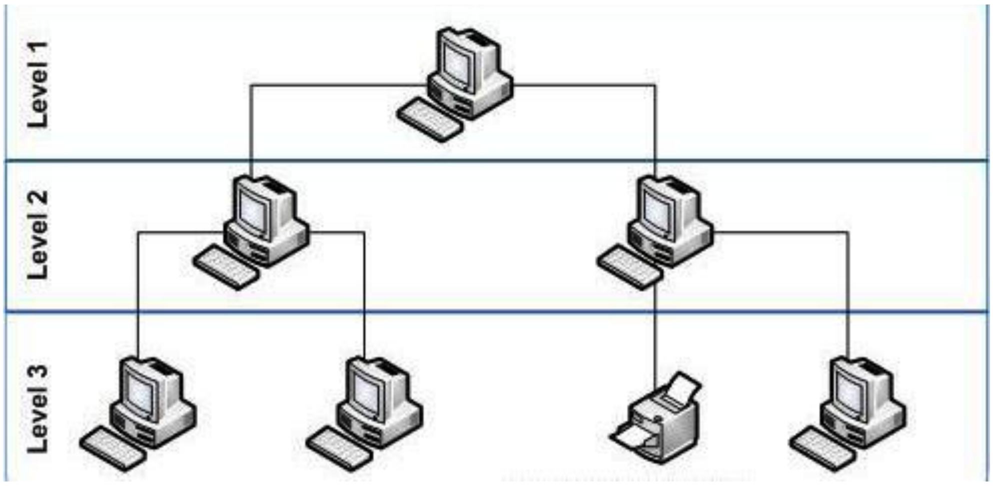


Figure 2.2: Tree (hierarchical) Topology

Advantages [2]:

- It is a reliable alternative solution for star and bus topology. As they have many similarities in their operation, the tree topology can replace them in cases that more scalability is requested.
- New nodes can be added without any consequence about the administration of the network or about the operation of the rest network.
- There is the central node (root) but also the overall topology is distinguished in separate smaller tree networks (segments). This enables better management and control of the topology.
- If a segment fails does not affect the rest network.
- In a case of a damaged node or segment the recovery procedure or even replacement is manageable issue. Furthermore, a disoperation in the network can be detected easily.

Disadvantages [2]:

- The more expanded the network becomes the more difficult its management becomes

- If the root of the topology fails then the overall network is affected.

ADVANTAGES	DISADVANTAGES
More scalable	Root failure means network’s failure
Easy expansion	
Root and Segments provide better management	
Segment failure does not affect the total network	Network’s expansion could be unmanageable
Detection and recovery of malfunctions are manageable issues	

Table 2.2: Advantages and disadvantages of Tree topology

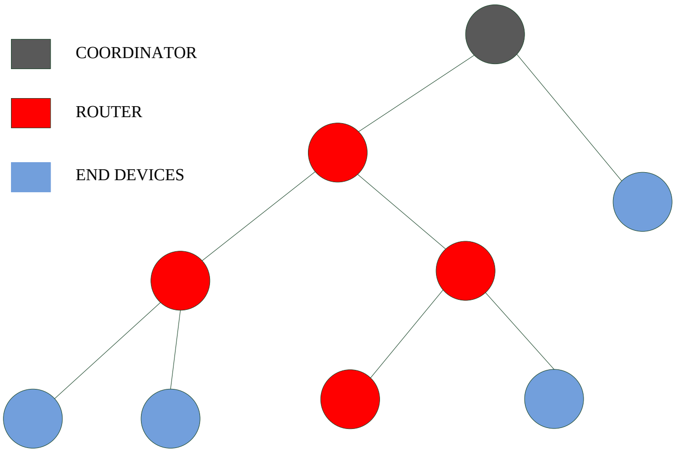


Figure 2.3: Tree topology

2.3 Mesh Topology

This is a topology that every single node that is part of the network is connected to the rest nodes through hopes (multi-hopping service). This main characteristic of the topology provides with a redundancy of paths the whole network. When a sender transmits data they follow a specific route according the algorithm that is implemented in the network and the protocols it uses. If a node that the route contains breaks down or fails there are numerous links to support and guarantee the network’s proper operation, the so called self healing capability which reassures the sender that the data will reach the receiver. To accomplish that there are algorithms and processes that run in order to find the alternative path so that the packets to be delivered to the destination (based on delay, traffic, bandwidth, number of remaining hops, cost and other parameters). Consequently, in this way the network behaves in a complete fault tolerance which is very important to organizations and corporations since the downtime is a serious issue for them.

In addition, in this way congestions are avoided because the availability of many different segments enables flexibility as far as the routing is concerned. In order for the congestion to be avoided there are, also, mechanisms and processes that can coordinate or synchronize the transmission of the nodes according to a time scheduling [19].

As we can realize in a mesh topology all the nodes are equal and so it is their participation to the network, too. There is not any master or central node to control everything happens in the network, preventing the instant exchange of information among the nodes of the network. However, this type of networks is not preferred since their implementation is very demanding and especially complex. What is more, mesh topology provide efficient solution being resilient in case that a node fails but does not serves helpfully about its recovery. If control or monitoring devices of the network do not exist then the broken node cannot be noticed and repaired.

There can be two different types of nodes, in a mesh topology, the Base Station (BS) and the Subscriber Station (SS). The BS is responsible for a communication between two different mesh topologies to take place. It is the node that will contact to an external node of the topology and will exchange data with it. It cannot be done by every single node in the topology because then we will have an infinite mesh network without computational efficiency and utility. Moreover, the topology can be divided in neighborhoods and extended neighborhoods. A neighborhood for a node is the total of the rest nodes that data can be exchanged with just one hop. These nodes called neighbors. Including the neighbors of these neighbors we have the extended neighborhood for a node.

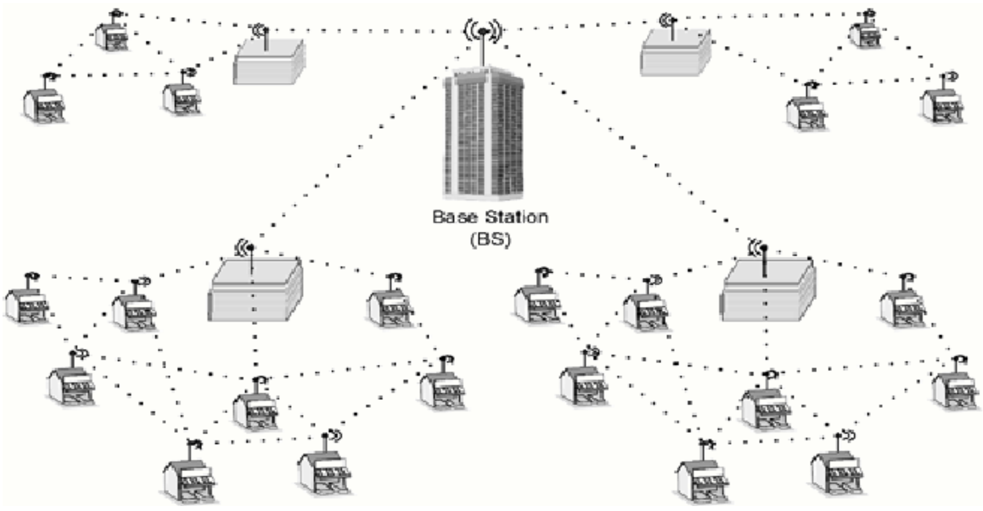


Figure 2.4: Mesh topology

Advantages [2]:

- The redundancy of hopes provides with many alternative solutions in case that the preferred one cannot be followed
- That has as a consequence the second very important advantage of this topology, the fault tolerance. If a node fails then the transmission is not blocked, but the data reach their destination
- The addition of a new hop does not affect the rest nodes and the network's operation at that time.
- The absence of a central node eliminates the chances of an overall failure of the network.

Disadvantages [2]:

- A mesh network topology could be expanded enough. This would demand great costs to be managed, to be controlled and monitored, so it may be unaffordable.
- Due to the multi hopping mechanism often delays could be noticed among the devices.
- It is a difficult task to be established and its initial coverage to be planned.
- Troubleshooting is a difficult issue in this topology especially in case a node breaks down.

ADVANTAGES	DISADVANTAGES
Redundancy of hopes	Uncontrolled expansion
Fault tolerance	End to end Delay
Flexibility in new hops	Difficulty in planning
Absence of a central node	Undetected broken nodes

Table 2.3: Advantages and disadvantages of Mesh topology

2.4 Protocols used by commodity smart meters

In this chapter there is an analysis in some routing protocols that can be used in mesh networks. Two categories of these protocols are mentioned:

- Reactive
- Proactive

Reactive protocols: In these protocols there is the demand of continuous updates as far as the overall topology of the network is concerned. In this way, every single node is able to calculate the most efficient route before transmitting its data. If there is not traffic generated by the nodes then there is no routing at all. A reactive protocol can discover, maintain and delete a route while the packets’ forwarding is taking place either within source routing or hop by hop.

Proactive protocols: The major advantage of these protocols is that there is a directly available route to every destination consequently delays are decreased. These protocols are based on the Distance Vector and Link State algorithms combining their characteristics. Additionally they optimize the flooding technique within the network

2.4.1 Open Shortest Path First (OSPF)

It is a protocol of internal dynamic routing which uses the flooding method to transmit and Dijkstra algorithm to calculate the paths with the minimal cost. There is a Link State Advertisement (LSA) in every router, which is actually a data base where there are updates about other routers’ LSAs of the Autonomous System (AS). Each LSA contains information about link cost factors. These factors are external metrics that define which link will be preferable based on throughput of a link, delays (as a delay could also be considered the distance of the nodes) and the reliability. The routers exchange LSAs and each one of them saves these information in its data base, the Link State Data Base (LSDB). In this way a flooding of the network is taking place so that every router can be able to depict the overall network's topology while the LSDBs are absolutely synchronized. Having updated the LSDB every router can calculate the shortest path within the network for specific destinations minimizing the link cost. These paths form the routing table of every node [3].

Algorithm

In a network with K nodes, the total amount of the periodic transmitted messages will be K^2, since every node transmits LSA to the rest ones. As a result there is a respectful limitation of the available bandwidth. To avoid this impact there are designated routers which receive the messages of the nodes and is responsible to deliver them to the rest nodes reducing the total transmitted messages to 2xK. Moreover, in this way every node's LSDB is synchronized according to the designated router. In case the designated router fails there is an alternative one which takes its place when this disoperation is detected.

Moreover, there is the possibility a network, if it is very expanded, to create huge data bases to each router and consequently there will be the need of more memory and calculating power to be implemented which demands more costs. To avoid that, the OSPF protocol divides the overall network in smaller areas to facilitating the resources' management and making the network more efficient. Every area has a kind of independency meaning that the nodes of every area are synchronized internally and not regarding the overall network. Moreover, the topology of every area is not visible to the rest ones therefore the routing information is reduced drastically across the network. The communication among the different areas is achieved within the connecting routers. These routers maintain one different database for every area that they serve. What is more, there are routers that exchange information with external networks.

Finally, there is the backbone area (the core) of the network, 0-area, where every single area has access although without having the ability to know details about the topology of the backbone. Every single area should be connected to the backbone. However, it happens due to the network topology some areas not be able to contact directly with it but to use another area as an intermediary. In this way, the remote area transmits its traffic through an area directly connected to the backbone, establishing a virtual link to the backbone. This remote area can be characterized as isolated area since it has one input and output gateway which is its intermediary and that is because these areas cannot play the role of their intermediaries. More specifically, an isolated area cannot be used to as a virtual link for another area so they communicate with the rest network sending their traffic only within their virtual link [3], [4].

Messages and operation

A router in order to establish a connection with its neighbors transmits a message HELLO. The same message receives from the neighbors as a response, registering the operational neighboring nodes with which exclusively will exchange routing updates.

In case that there are more than 2 routers in an area, one router is defined as the designated router (and another one as the alternative designated router) which connects with the rest ones (relationships) exchanging routing information in order to synchronize them. Since the synchronization is completed, the routers execute the Dijkstra shortest path algorithm creating a tree with root themselves towards the total known destinations. Thus, they explore the best forwarding route for every destination. Then they LSAs and transmit periodically HELLO messages to check and verify the neighboring routers topology and status. If a router discovers a failure node then it informs everyone else enabling them to update their data bases [3], [4].

2.4.2 Optimized Link State Routing (OLSR)

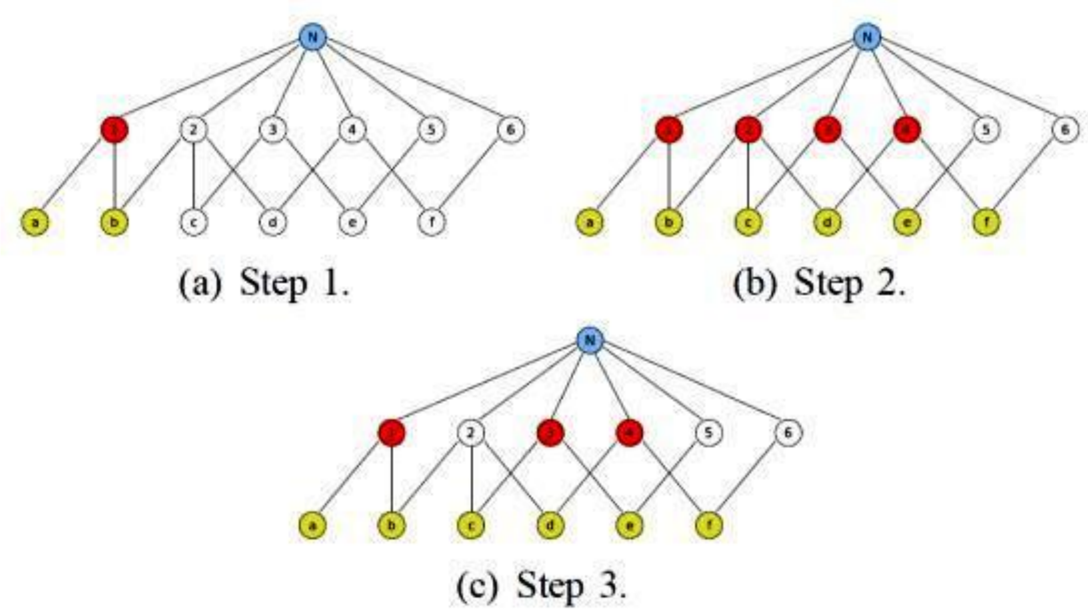
It is a table driven protocol exchanging continuously information with the rest nodes regarding the network's topology. This protocol minimizes the possibility of the network's overflow using selected nodes to transmit broadcast control messages, which are known as multipoint relays (MPR). Every single node in the network chooses a number of nodes as its MPRs in such a way that the total MPRs to cover the whole nodes that are two hops apart from itself. The less the MPRs are, the less the overhead is due to the traffic control.

More specifically, every single node transmits periodically HELLO messages to discover its neighbor nodes. These messages are received by the 1-hop nodes and are not forwarded further. Consequently, every single node can select as many 1-hop nodes as MPRs in order to be able to communicate with the 2-hops nodes.

Algorithm:

1. Suppose one node N which must select its MPRs every neighbor node which is single neighbor of a 2-hop node.
2. Then selects as an MPR a neighbor node that covers the majority of the 2-hops nodes that do not communicate with the rest MPRs of the node N.
3. Finally, node N excludes from MPRs the neighbors that are not necessary for a communication among node N and the 2-hops nodes to be established. Actually, if a neighbor node stops being MPR and the node N still can contact with every single 2-hops node then it is excluded totally from MPRs.

The algorithm is depicted below in the Figure 2.5.



(a) Step 1.

(b) Step 2.

(c) Step 3.

Figure 2.5: OLSR Algorithm

- Step1: The node N selects the node 1 since it is the only node that can communicate with the 2-hops node a.
- Step2: The node N selects successively the node 2 since it covers 2 unknown until that time 2-hops nodes c and d, the node 3 to cover the node e and the node 4 for the node f. As a result all the 2 hops nodes are covered with the selection of 1,2,3,4 nodes as MPRs.

- Step3: The node N excludes node 2 from a MPR since even without him all the 2-hops nodes are still covered. Therefore the node N has as MPRs the a, c, d nodes

Topology recording

Every single MPR node transmits a Topology Control message (TC message) every TC interval (update period) in order for every node to be informed about the network's topology. In this TC message from a MPR node it is included which nodes have chosen this specific node as their MPR. The TC messages are transmitted across the whole network and they are using MPRs to reduce the number of transmissions. To optimize the flooding the following rule is implemented:

- Every node N forwards a message only whether it is received for the first time by a node that has chosen N as its MPR.

Thus, every single node is accessible either directly or through its MPRs. The information about the neighbors and the network's topology is updated periodically, allowing each node to calculate the routes towards the overall known destinations. This is happening using shortest path algorithm of Dijkstra.

2.4.3 Destination Sequenced Distance Vector (DSDV)

The DSDV protocol is based on the Bellman-Ford routing algorithm. According to this protocol, every mobile node has a routing table where it buffers every possible destination, the required number of hops for each destination and the sequence number as it is defined by the source. The sequence number is for the old routes to be diversified form the new ones so that possible loops to be avoided. In this way DSDV consist of updated routes. The nodes transmit periodically their routing tables to their neighbor nodes (1-hop nodes) to update the routing tables. Among these transmissions, they are able to transmit their routing tables if an important change happens to the network topology and consequently to their routing tables. Such updates could cause a great amount of traffic to the network. To decrease such traffic, these updates can be sent in the following ways:

- “Full damp” packets: they contain entire the routing tables and they can demand many data units from the Network Protocol Data Unit.
- Incremental packets: they contain the records that have changed since the last update and they demand only one data unit from the Network Protocol Data Unit reducing drastically the generated traffic. If the incremental packets are large enough then they can include that records whose sequence number has changed.

When there is a stable network then incremental packets are sent while full dump packets are rare. Otherwise, full dump packets are more often than the incremental ones.

Every update packet contains destination IP, the number of hops so that the packet to reach the destination, a sequence number relative with the received information regarding this destination and a unique sequence number of the transmission. The last received route, this one that has the bigger sequence number, is the preferable one. In case two routes have the same sequence number then the one with the smallest number of hops is the preferable. If all the metrics are equal then the selection is random.

When a node N realizes that a route until a final node K is not valid then the number of hops for this route increases. The next time the node N will announce its routing table to its neighbors, will lend to the route towards K an infinite number of hops and a larger sequence number. When the nodes decide which the best route to be selected is, they include at the total time the average time that a route needs to be published (setting time) reducing in that way the network’s traffic.

Disadvantages

1. The setting time does not have efficient results in the mesh networks. That is because we await in a mesh network the topology changes continuously so the setting time instead of reducing the network traffic has as a result a considerable number of packets to be rejected for transmission because a route has not be selected.
2. The periodical transmission of the updates, no matter if any change in the network’s topology has happened, limits network’s expansion since more nodes will aggravate the total cost.

2.4.4 Ad hoc On Demand Distance (AODV)

Aodv is based on the Distance Vector Algorithm and it could be characterized as an improvement of DSDV as its main characteristic is that it publishes routes when it is required and not periodically. In that way it minimizes the transmissions and the generated traffic in the network.

Every single node in the network maintains a routing table where every record consists of the following elements:

- Destination IP, sequence number
- The required hops number of the route
- Next-hop index
- Time To Live (TTL) of the route
- Request Buffer
- Neighbor nodes that are included in the route

When a source wants to send a packet to a receiver begins a procedure of finding a path to detect the destination. Initially, it transmits a route request (RREQ) to its neighbors. The same their neighbors do, they transmit the packet to their neighbors and so forth and so on until it reaches a node that has a recent route for the destination or the destination itself. Each node drops a repeated RREQ.

The sequence numbers of destinations are used in order to prevent routes to have loops and to reassure for the proper updating of the routing table. There is a different sequence number for each node and an ID transmission, as well, which increases every time a RREQ is sent by the node. The ID transmission and the node's IP address predefine in a unique way a RREQ. In a RREQ it is included the source's sequence number and also the last received sequence number that has for the destination. Intermediate nodes can answer to the RREQ if they have a route for the destination with a greater sequence number which means that this route is the soonest update for the destination. In this way, we can be sure that the route was used recently and successfully meaning that there were not any loops within it. However, if there is not synchronization among the sequence numbers then great problems could be caused to the network's operation.

During the forwarding of the RREQ each node records in its routing table the neighbor node that sent the RREQ in order to be able to form the reversed path to transmit back the Route Reply (RREP). A RREP is unicasted either by the destination or by an intermediate node that has a greater sequence number for the destination. As the RREP propagates, the intermediate nodes record in their routing table the route towards the destination. When the source receives the RREP can begin transmitting data. If the source does not a receive RREP then it can either retransmit a RREQ or suppose that there is no route for this destination. The RREQ and RREP instructions have the role of discovering the route for a message to be delivered and they do not increase the network's overhead.

If nor RREP is received that means that one (or more) node, which is included in the route either as intermediate or as the destination, is broken or moved, so the topology has changed. In this case, the previous node from the dismissed one in the route sends a Route Error (RERR) to the source recording the overall nodes which are not accessible due to that disoperation. This message is sent hop by hop to the source sharing the included information to the rest active nodes of the route. The source when receives the RERR restarts a procedure of finding the new route for this destination.

Another alternative operation is the use of "HELLO" messages which are sent from a node to all the 1-hop nodes, its neighbors. In this way every node can know exactly which nodes are active around it in order to update its routing table. In this way the route maintenance is accomplished and the messages do not generate additional overhead to the network.

The difference with the AODV algorithm with Distance Vector or Link State or other algorithms is that it reduces drastically the routing messages across the network. Therefore, there is limited traffic regarding to the control messages but there is increased latency by finding new paths. In addition, if a node has recorded the active nodes around it optimizes the total overhead of the network. Moreover, it is a flat routing protocol so the need of a central node to maintain the network is not necessary. However, if a connection failure occurs across a route then AODV should be called again from the source and the new route to be discovered to reach the destination. There is not the facility the intermediate nodes to be allowed to reroute the initial path in order for the packet to be received. Thus, great time margins are needed to reestablish the proper route.

3 Analysis of RF mesh protocols

3.1 Carrier Sense Multiple Access (CSMA)

Multiple Access Schemes are techniques that can assign channels to multiple users within the given portion of the frequency spectrum (dividing limited radio resource amongst multiple users)

Carrier Sense Multiple Access (CSMA)

There are 4 CSMA access models:

- 1-persistent
- Non-persistent
- P-persistent
- O-persistent

3.1.1 1-persistent CSMA

When a station has data to send, listens to the channel (medium) to be sure that no other station is transmitting. If the channel is busy then it waits until the channel to become idle. When the station senses that the channel is idle then transmits a packet. If a collision happens then the station is waiting for a random back off time repeating the same procedure. The station senses idle channel transmits with possibility p=1 that is why it is called 1-persistent.

Transmission delay has an important impact on the way the protocol performs. There is a small possibility that just after one station begins sending its data a second station to be ready to transmit (almost simultaneously). If the signal of the first node is not detected by the second one then both sense an idle channel and send their packets creating collision and interference. The more the transmission time is the greater this problem becomes the less efficiently the protocols performs.

Even if the transmission delay was zero the above problem is probable to happen. If two nodes want to transmit but the channel is busy they are going to wait for their chance. However, the awaiting time will make them impatient and when they will sense an idle channel they will send their data simultaneously ending up with a collision across the medium.

3.1.2 Non-persistent CSMA

This access model is less greedy than the previous one. Specifically when a station is ready to transmit before doing so, it listens to the medium and if no one else is going to send anything then it can begins its transmission. If the sender senses that the medium is busy then it waits. The difference is that now the sender does not detect continuously the medium so that it starts sending its packets the time that the current transmission ends. Instead, it waits at a random back off time and then repeats the same algorithm.

This protocol is more efficient as far as the utilization of the medium is concerned since the possibility of collision is tiny this time. However, the negative is that there are greater delays comparatively to the previous access model.

3.1.3 P-persistent CSMA

This protocol is implemented to the channels with a kind of slots. When a station is ready to transmit listens to the channel. If it is idle, transmission is taking place with a probability p. With a possibility q= 1-p the station can abort the transmission and for the next available slot. If the next available slot is also idle then the station can either sends the packets or abort it again with possibilities p and q respectively. This procedure is being repeated until the whole sender's data (frame) to be transmitted or one other station uses the channel. In this case, another node using the channel, the station that was to transmit acts as it would if a collision had happened, waiting a random back off time and starts the same procedure from the beginning. If the station senses a busy channel then waits for the next available slot and implements the same algorithm again.

3.1.4 O-persistent

This protocol operates like a queue that serves the packets in order giving in its one its own slot to be served. Actually, there is a supervisor station that gives a transmission order to each station. According to this order each one waits for its time to transmit. The station that was chosen to be first begins immediately to transmit. The second one waits for the next time slot while the first station is transmitting. In this way all the stations of the network are informed for the current transmissions and adjust their assigned order getting closer to the slot that will be dedicated to each one of them so that they can transmit their packets.

3.2 Carrier Sense Multiple Access / Collision Avoidance (CSMA / CA)

In this protocol the detection of the physical and also of virtual channel is used. CSMA/CA operates in two different methods.

In the first method, when a station is ready to transmit, detects the channel. If it is idle, transmission is taking place. During the transmission, the station does not detect the channel but sends entire the frame which could probably received damaged by the receiver due to interference at the receiver's side. If the channel initially is busy then the transmission is cancelled until it becomes idle again. If a collision occurs among stations then these stations await for a random back off time, using the binary exponential backhaul algorithm (After mth collision, Network Information Centre(NIC) chooses K randomly from 0,1,2,3…2^{m}-1. NIC waits K*512 bit times, starts from scratch.

In the second method, there is detection of the virtual channel. As it is shown in the Figure 3.1, station A wants to send to station B. Station C is out of B's range (and possibly in the range of A's but that is not important to us). Station D can listen to B but is out of A's range, too.

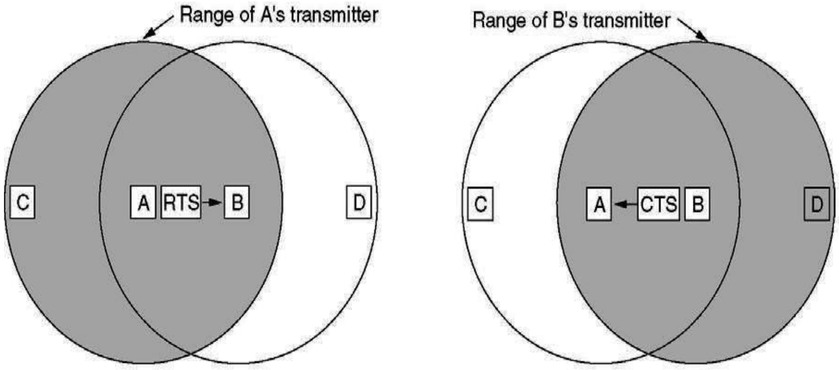


Figure 3.1: CSMA/CA Method 2

Suppose that A wants to send data to B. First of all, A sends a Ready To Send (RTS) frame-query asking for B's permission to start transmitting. When B receives that request if it wants receive data from A sends a Clear To Send (CTS) frame. When A receives the CTS frame, the RTS-CTS handshake is set and A is able to send the packets it wanted to, waiting a timetabled acknowledgement as reply from B. When B receives properly all the packets sends back an acknowledgement to inform A and the RTS-CTS handshake to be completed. If the time that was set by A about the ACK before it ACK received then entire the packet is transmitted again.

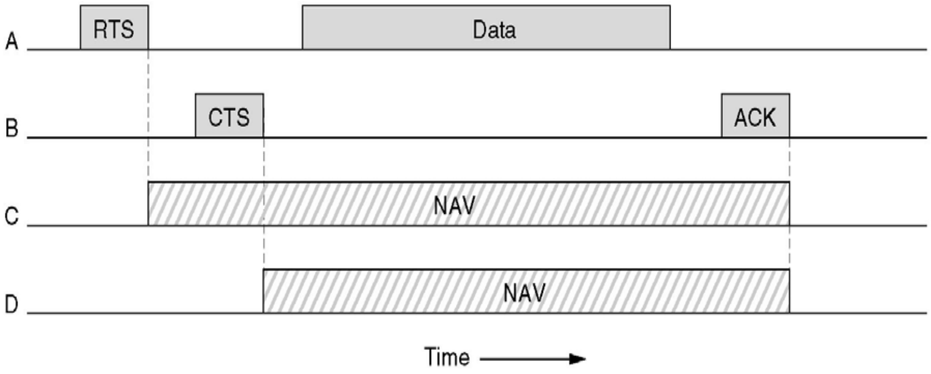


Figure 3.2: Detection of virtual channel with CSMA/CA [20]

Let’s examine this handshake from C and D point of view. C senses A therefore could receive the RTS frame. In this way it realizes that in a while there will be exchanged information between two nodes so avoids of transmitting anything until the handshake to be completed. By the included information in RTS C can calculate approximately the duration of the handshake including the final ACK knowing how much time the channel will be busy if nothing goes wrong. This time is shown in the figure as Network Allocator Vector (NAV).

Station D does not sense the RTS but senses the CTS frame, in that way enables a respective NAV which lasts less time than C’s NAV. NAVs are not transmitted; they are internal notifications which inform their station the time duration that they should remain silent without transmitting.

In wireless networks the Signal to Noise Ratio (SNR) has a crucial role and that is happening due to many phenomena and devices such as the micro wave ovens that transmit in the same frequencies. Consequently, the possibility for a frame to be received properly is reducing according to frame’s length (the longer a frame is the smaller its possibility is for it to be transmitted successfully) [6].

The CSMA/CA algorithm needs three variables to be available every time that a device tries a transmission [5]:

- Number of Backoffs (NB): it records how many times a node was forced to backoff for a specific transmission. Initially before any transmission it is equal to zero.
- Congestion window: defining the number of backoff periods that need to be clear of channel activity before the transmission can commence. Every single time that a node wants to transmit data the value of the congestion window should have as an initial value the number 2. This should also happen when the channel is busy aborting the transmission of data for a node.
- BE: It is the backoff exponent which indicates the number of the backoff periods that a node should not transmit until it is able to try a new transmission listening to the channel. This period of time that a node waits to the backoff window is among 0 and 2^{BE}-1.

The CSMA/CA algorithm is implemented using a basic time unit called Backoff Period (BP), which is equal to aUnitBackoffPeriod=20 symbols (0.32 ms)

More specifically, below it is described the procedure that the algorithm follows [5], [6]:

1. The Mac layer initializes the Number of Backoffs, the Congestion Window and the Backoff exponent and then locates the next backoff period. The Backoff exponent getting started with the MACMinBE which is a constant defined by the 802.15.4 protocol and it is equal to 3.
2. The MAC sublayer is waiting for a random number of backoff periods in the range of 0 and 2^{BE}-1 to avoid collisions.
3. Since the backoff delay is completed, the MAC is waiting for an idle channel to be provided by the Physical layer. The algorithm runs a Clear Channel Assessment (CCA) procedure equal to 8 symbols (0,128 msec) in order to evaluate the channel's activity. In case the channel is idle the algorithm goes to step 5, otherwise to step 4.
4. In case the channel is not idle, the MAC sublayer will raise by one the number of backoffs and the congestion window while the backoff exponent must not become greater than the maximum backoff exponent (which is predefined as MACMaxCSMABackoffs=5). Congestion window becomes 2. if the value of the number of backoffs is less or equal to

the maximum number of CSMA backoffs the procedure is repeated form the point 2. If it is not, the algorithm is terminated with a Channel Access Failure status.

5. If the channel is determined to be idle, the mechanism should ensure that congestion window is equal to zero and that is when the Mac transmits its packets. If it is not the procedure is repeated from the point 3. Despite the transmission is able to begin, collisions are possible to happen whether two or more nodes start to transmit simultaneously.

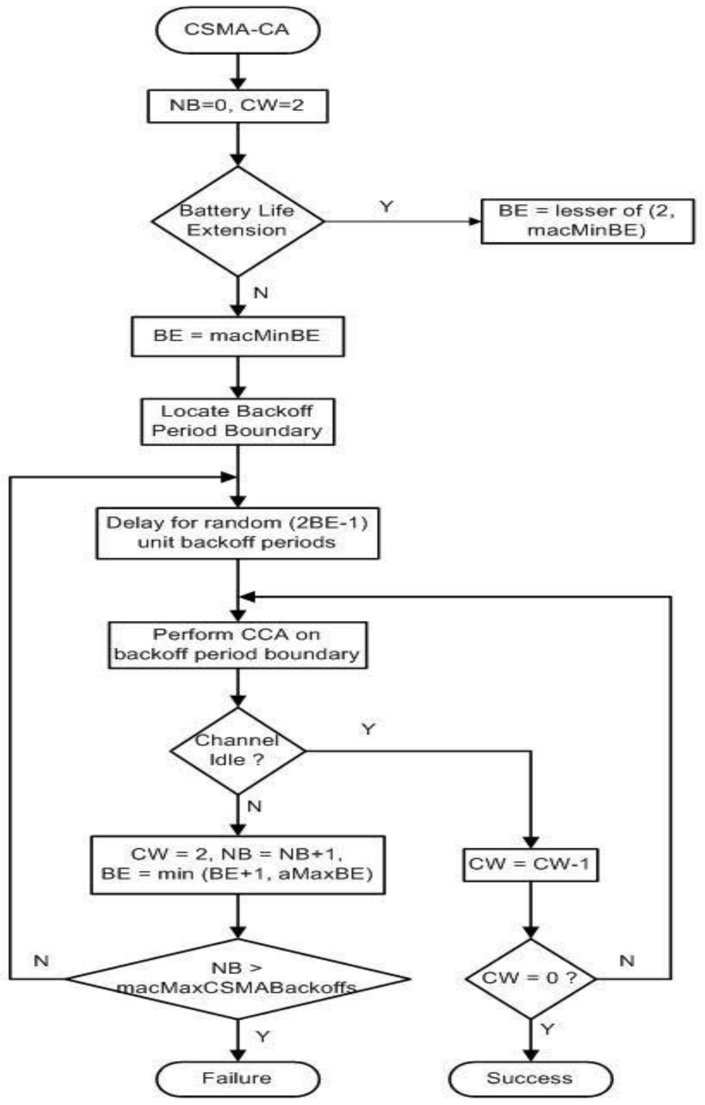

CSMA-CA
NB=0, CW=2
Battery Life Extension
Y
BE = lesser of (2, macMinBE)
N
BE = macMinBE
Locate Backoff Period Boundary
Delay for random (2BE-1) unit backoff periods
Perform CCA on backoff period boundary
Channel Idle ?
Y
N
CW = 2, NB = NB+1, BE = min (BE+1, aMaxBE)
CW = CW-1
N
NB > macMaxCSMABackoffs
CW = 0 ?
N
Y
Y
Failure
Success

Figure 3.3: CSMA/CA datagram [5], [6]

The major advantages of CSMA/CA are that the problems of hidden terminals and exposed terminals are overcome.

Hidden Terminal problem

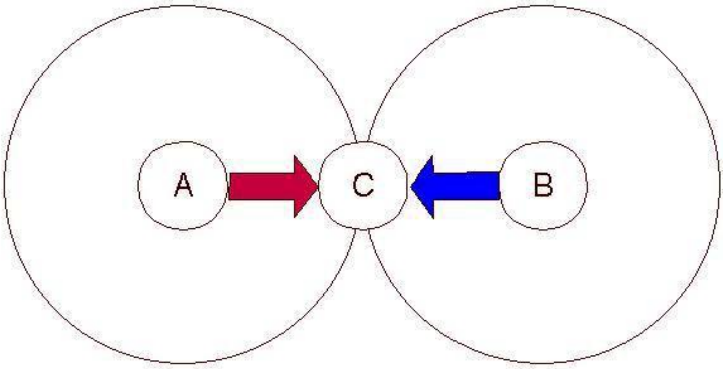


Figure 3.4: Hidden Terminal problem

As it is shown in figure 4 both A and B stations want to share information to the C station. Suppose that A first sends a RTS frame to C. Since C is idle transmits a CTS frame accepting A's request. B cannot detect the RTS request since it is out of A's range therefore it can detects only C's activity. B sensing the CTS transmission by C is not allowed to send to C its data since the channel is busy. When the communication between A and C terminates then B can transmit to C.

Exposed Terminal problem

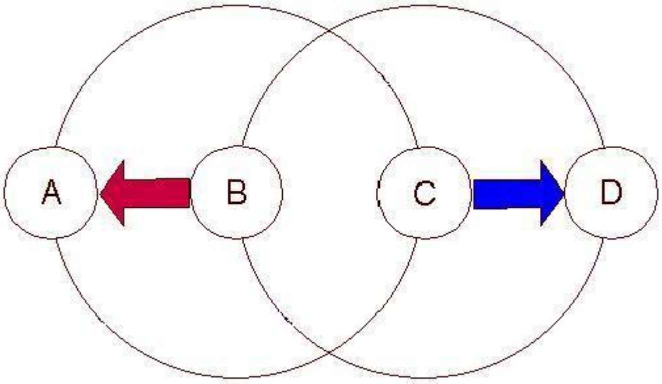


Figure 3.5: Exposed Terminal problem

In this problem there is a totally different situation. B wants to communicate with A and C wants to communicate with D. B to set the RTS-CTS handshake with A transmits a RTS frame. Meanwhile, both A and C receive that frame. However C realizes that this frame is not destined for itself and neither for D station. What is more, C is not going to receive any CTS frame from A since it is out of A's range. As a result C is not necessary to wait for A and B to end up with their communication. Instead it is allowed to contact to D setting their RTS-CTS handshake.

3.3 ZigBee protocol

ZigBee protocol was generated by the cooperation of many companies (ZigBee Alliance) trying to construct wireless control and monitoring-observation devices. ZigBee protocol was based on IEEE 802.15.4 which has a lot of compatibilities with. The main characteristics of ZigBee protocol are:

- Low data rate 20-250 kbps
- Operates on the unlicensed frequency range of 868 MHz, 900-928MHz and 2.4 GHz
- Low range 10-100 m
- Low power consumption
- Employs 128-bit AES encryption type
- Provides with reliability and cost effectiveness

3.3.1 Protocol stack

ZigBee was built on the top of the IEEE 802.15.4 layers and was targeted to the four following layers:

1. Physical layer
2. Medium Access Control layer, MAC
3. Network layer
4. Application layer

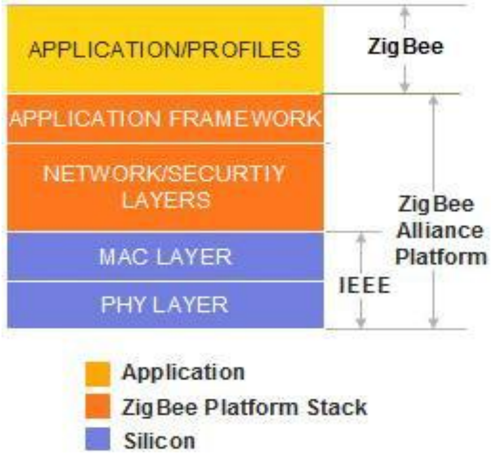


Figure 3.6: Protocol Stack [8]

The ZigBee protocol stack provides the opportunity many devices to be interconnected in the same network. Additionally, the protocol is constructed in such a way that is very tolerant to similar RF devices [8], [11].

The Physical layer (PHY) is responsible for the enable or the disable of the transceiver, for the data to be transmitted and received, for the evaluation of the current situation of the channels to implement CSMA/CA and for the recording of the received packets' quality. At this layer ZigBee uses Direct-Sequence Spread Spectrum (DSSS) with two different Phase-Shift Keying (PSK) modulations so that interference to be minimized.

The Medium Access Control layer (MAC) provides services of transportation and management of the packets. It is responsible for the channel's access and for a reliable connection between two MAC layers. Additionally, it contains the necessary procedures for the security mechanisms to be implemented [9],[10],[11].

The Network layer (NWK) is responsible for the management of multi-hop communication bridging the ZigBee and IEEE 802.15.4 protocols within the Network Layer Data Entity-Service Access Point (NLDE-SAP) and Network Layer Management Entity-Service Access Point (NLME-SAP) interfaces. NLDE-SAP is responsible for the datagrams, creating the appropriate packets according to the received data from the upper layers and deciding for their correct routing across the network. NLME-SAP deals with procedures such as the implementation of new network, the detection of the neighbor nodes, recording of routing messages, new devices' addressing and selection routing mechanism.

The Application Layer is the top and the most complex layer and it consist of:

1. The Application Framework which is actually the executive environment for application objects and where the data that run in a device are sent and received. Every application object has access to the framework within the endpoints or ports (the number of endpoints is 1-240).
2. The ZigBee Device Object (ZDO) which is an application object placed in the port 0 and it is executed always first before every device. This is the object that determines devices' roles (router, coordinator, end device) and initializes the Application and Network layers. It deals with the assessment application services that every device has to provide with and the management of the security services.
3. The Application Support Sub-Layer which settles the routing tables that are placed on the coordinators and the routers. They contain the source IP address and port and also the destination IP addresses and ports. This layer describes how the ports operate and the data requests and acknowledgements that are used.

3.3.2 Routing

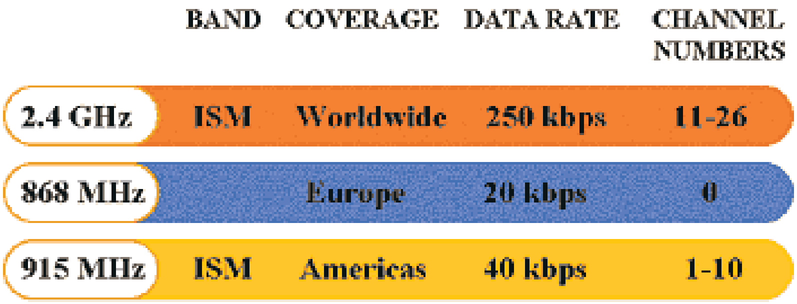
The simplest way for routing messages in Sensor Network is flooding. Each node transmits its measurements to its neighbors which acting in a same way until the initial packet reach its destination. It does seem to have high simplicity, although it has a serious disadvantage that of overloading the network with packets without final destination which traversing continuously across the nodes resulting in an extravagant consumption of energy and resources.

The most common routing algorithm is the Ad-hoc On Demand Distance Vector (AODV). Every node processes information about the possible routes to the destination forming the routing table. The routing table contains ID number destination, number of remaining hops, transaction cost and the ID number of the next included hop in the route. At the same time, AODV is informed about the traffic of the network in order to be able to save energy and to minimize the use of the remaining resources.

The routing table is updated with every new entrance (a new node included in the network). The new node sends a connection request to the neighbors and they send a number of alternative routes back to it. More specifically, a neighbor node after the received request sends the current route of its routing table. The new node will join the network within the node that has the minimum number of hops for the destination. In case that a node breaks the forwarding stops and the procedure restarts. The disadvantage with this algorithm is that it needs much time for joining a new node in the network since there has to be correspondence by all the existing nodes in the network.

3.3.3 Reliability

The reliable data transmission is very crucial in ZigBee applications. The 802.15.4 protocol which is liable to ZigBee provides this reliability within different mechanisms in multiple layers.



	BAND	COVERAGE	DATA RATE	CHANNEL NUMBERS
2.4 GHz	ISM	Worldwide	250 kbps	11-26
868 MHz		Europe	20 kbps	0
915 MHz	ISM	Americas	40 kbps	1-10

Figure 3.7: 802.15.4 different frequency ranges

As it is shown in the Figure 3.7, 802.15.4 uses 27 channels in 3 different frequency ranges that are provided. There are differences across the countries concerning the use, the propagation, the losses and the data rate which enable the constructors of the ZigBee to optimize its performance.

The range of 2.4 GHz is used worldwide, it has 16 channels and supports data transmission with the maximum of 250kbps. The 902-928MHz provides America and many coasts of the Pacific Ocean 10 channels with the maximum of 40kbps. In Europe it is used one channel in the range of 868-870MHz at 20kbps. In a specific channel the transceiver 802.15.4 is based in a summation of mechanisms to verify reliable data transmission. Initially, the physical layer implements Binary Phase Shift Keying (BPSK) modulation at 868-915 MHz and Offset Quadrature Phase Shift Keying (O-QPSK) at 2.4GHz. Both modulations operate efficiently in environments with low SNR (Signal to Noise Ratio). The encoding in the carrier is done with Direct Sequence Spread Spectrum (DSSS) technique which optimizes the multipath performance and the receiver’s gain as well [11],[12].

3.3.4 ZigBee Datagram

It is very important for the proper and effective transmission of the information in the ZigBee protocol. In the MAC protocol data unit the payload consists of the source and the destination IP address, a sequence number that enables the receiver to identify that every sent packet has been received, frame control bytes and frame control sequence that verifies that no losses exist. This MAC frame is included in the in the synchronization header and the PHY header of the physical so that it enables the receiver to identify and decode the received packet. Then the receiver executes a 16-bit cyclic redundancy check (CRC) to verify that the packet was not corrupted. In case the packet was transmitted correctly the receiver sends back an ACK packet to inform the sender that the transmission was completed successfully. Otherwise, the receiver drops the packet without any notification and the packet is retransmitted until a notification is sent back. If the route between the source and the destination is not reliable any more or is broken, the ZigBee protocol provides with recovery mechanisms the network in order for alternative routes to be implemented.

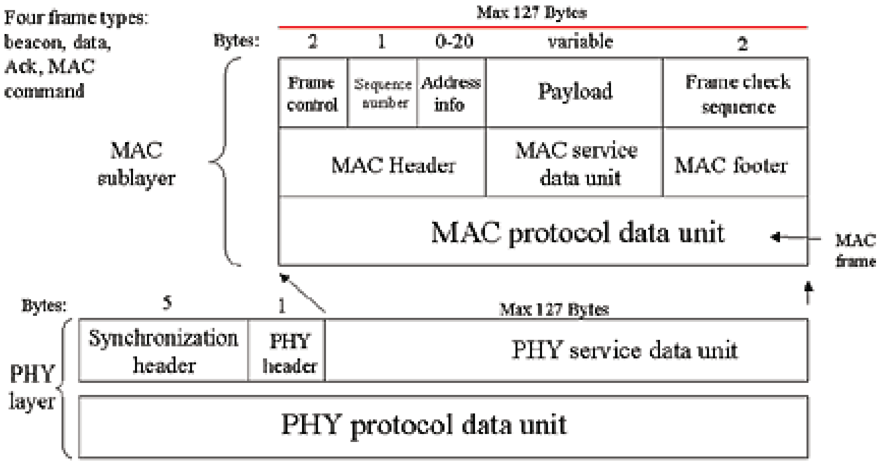


Figure 3.8: ZigBee Datagram [12].

3.3.5 Voltage

In the networks where ZigBee protocol is used, a node consists of a CPU, a buffer, contact devices and input/output devices. However the most important in the nodes is the device that provides the node with the necessary energy, for example a battery. In order for the whole network to be installed and for the different devices to communicate with each other it has to be predicted and calculated the exact finite amount of energy that every node will need to operate properly. This will support efficiently the expansion of the network, too.

More specifically, we will examine the alternative options of energy generators that we have. The alkaline batteries AA type can support the capacity of 2850 mAh. A LED lamp consumes about 6mA. This lamp will be turned on for about 20 days and at the last days its lightning will be paler as the voltage is getting lower than 1.5V. As far as the solar energy is concerned, a PV of 30cm^2 is able to produce 40mA at 4,8V and about 6mW/cm2 in a line of sight, with this performance to be updated and improved during the passage of the years.

While a node is transmitting a message, consumes power of 35mW. The demanding energy for a message to be transmitted in a distance d is analogous to d^n, where the n varies. Nevertheless, the receiving is done constantly and its cost is increasing. Suppose that the recent motes consume 38mW of power waiting for the messages. As we can see the real cost in the wireless communication is not at the sender's side but at the receiver's.

Suppose a CPU that consumes 3mW power to process an instruction at a clock of 4MHz. It will need energy of 0.75nJ per instruction. In order for a transceiver to transmit or receive a bit, it consumes 35mW at 250kb per channel, it will need 140nJ which is almost two hundred times more energy. Consequently, in a network where the cost is the one that just described we have 3mW for the CPU and 38mW for the transmitter which is 41mW totally. This cost can be supported by an AA battery for a week. Of course this is not efficient at all for a wireless network.

3.4 Z-wave

Z-Wave is a Radio Frequency (RF) low power wireless communication protocol generated by Zensys corporation and Z-Wave Alliance. It is designed in such a way in order to be able to support home devices since it has except for low power and small range, too.

3.4.1 Technical Features

First of all, how Z-Wave works in a network. In order for such a network to be established, a controller and one controlled device (at least) are needed. A network's controller is not able to control a device until it is included in the network. That demands a specific sequence of buttons to be pressed on the controller. In this way the procedure of “adding” is completed and the device is recognizable to the controller. This sequence of initialization even if it is not so useful it is done only one time for the specific device. However, the procedure is repeated for every device that is included in the network so that it can be handled by the controller. A similar procedure is followed when a device is removed from the network and it is not enough just moving it out of the network or turning it off. The important in the Z-Wave network is that every device should have its final position before being included in it. This is happening because during the “adding” process, the controller calculates and buffers the power of the signal among the included devices and their move will affect these calculations [13].

The major characteristic of the Z-Wave protocol is its interoperability. It is based on a mesh network topology and despite its small range it could cover a whole floor. That is because 2 nodes in a network that Z-Wave protocol is used, can communicate even if each one is out of the other’s range, as long as a third (or more) node will be included in both ranges (the message is delivered with the hopping process). In case the nodes that act as intermediaries are broken, then the source node will try to find another path for the transmitted message to reach its destination successfully. That is why the majority of the nodes are also repeaters. That provides with great flexibility this protocol but also increases the transmission delays and it demands sufficient battery energy.

The main features of Z-Wave are summarized as follows [15]:

1) Simplicity of installation and deployment with automatic address assignment for the convenience of network management.

2) Lower cost.

3) Ultra low power consumption with the help of the lightweight protocol stack and compressed frame format.

4) Very small in size in terms of the hardware module for the benefit of integration with other devices.

5) Excellent in anti-disturbance with the support of two-way acknowledgement, random back-off algorithm and collision-avoidance.

6) Lack of potent mechanism that guarantees data security in communication.

3.4.2 Protocol Stack

The kind the Z-Wave operates gives great opportunities for many actions within the house to be more automated like the control of radio player, the control of the lights of the house remotely or even their synchronization with other devices like a DVD player, the control of the curtains or the thermostat remotely and the movement detection for alarm systems.

That is why the protocol stack of Z-Wave is built as it is depicted below

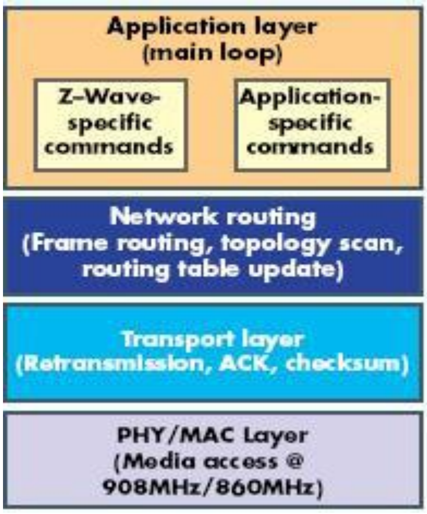

Application layer
(main loop)
Z-Wave-specific commands
Application-specific commands
Network routing
(Frame routing, topology scan, routing table update)
Transport layer
(Retransmission, ACK, checksum)
PHY/MAC Layer
(Media access @ 908MHz/860MHz)

Figure 3.9: Protocol stack [14]

Z-Wave uses the ISM band (860-916) in the Physical layer and also uses CSMA/CA to have access to the RF medium being in a busy situation preventing another node to transmit. Finally, it controls the medium using Manchester coding.

In the transport layer Z-Wave has the opportunity of data retransmission depending on whether or how on time an ACK will be received by the source node that will verify the successful transmission of the data. Moreover, it contains in this layer a checking mechanism for the detection of bit error rate of the packets.

In the routing layer the path that will be followed is formed according to the static location of the controller and the network's devices. The routing path includes the source, the destination and the devices that will be the hops in the routing path (the repeaters). It is not a static path since it can be dynamically adjusted regarding the current network topology and the current situation of its devices [16].

The application layer is responsible for the decoding and running the two types of commands that are shown above in this protocol

4 Networking a home and a neighborhood area with RF mesh

This chapter contains practical issues of this dissertation. We used Opnet Modeler 14.5 to run simulations as far as the Home Area Network and the Neighborhood Area Network are concerned.

We tried to identify the attitude of these Area networks based on specific parameters that can affect our topology in essentials operating factors. Consequently, we configured our networks' attributes according to the following:

- Topology: The main purpose of the simulations was to examine in which way each device of an Area Network transmits and forwards the data across the network so that they are delivered successfully to their destination. Therefore, we build our simulation to attend as:
  - Mesh network topology
  - Hierarchical Tree topology
- Position: Our investigation focused on how the nodes of the experiments should be placed in our simulator so that we could test and verify the optimality and tolerance of the network. Thus, the way that the devices were placed during the simulations were:
  - Randomly
  - In a Manhattan structure
- Data Rate: Two different values for this parameter were used to testify the manner every topology could be affected:
  - 500 bps
  - 20Kbps
  - 100Kbps
  - 1Mbps
  - 11Mbps

- Bandwidth: The included devices were configured to operate in 3 different bands:
    - 70KHz
    - 270KHz
    - 400KHz
- Frequency: The value of this parameter had to be for the Home Area Network at 868MHz since the ZigBee protocol is used at three specific ranges (868MHz, 915MHz and 2.5GHz). We have chosen that range since it is the one that approaches the 800MHz that the Neighborhood Area Network was simulated.
- Routing protocols: Two protocols were used that actually facilitate in a great manner our mesh topologies:
    - AODV
    - OLSR

PARAMETERS	VALUES
Topology	1. Mesh network topology 2. Hierarchical Tree topology
Position	1. Randomly 2. In a Manhattan structure
Data Rate	1. 500 bps 2. 20Kbps 3. 100Kbps 4. 1Mbps 5. 11Mbps
Bandwidth	1. 70 KHz 2. 270KHz 3. 400KHz
Frequency	1. HAN 868 MHz 2. NAN 800 MHz

Routing Protocols	1. AODV 2. OLSR

Table 4.1: Testified parameters

Building the Home Area Network we focused on ZigBee technology. Our purpose was to check the efficiency of this technology. So we have posed multiple combinations of the above parameters and trying to realize under which circumstances this technology could give us optimal and safe results. The time per simulation was 30 minutes. In every case, the coordinator is in a central position and the rest devices were placed around it. Besides, any other position for the coordinator would not serve our network in a better way, returning results that would be useless to us. Even though we experimented with that particular characteristic in order to be sure that a non central coordinator would not be able to share data across the network more sufficiently.

In Neighborhood Area Network we built a wireless LAN setting a sufficient number of nodes to operate under different routing protocols. We would like to test ZigBee but its specifications do not meet the requirements of such an Area Network. In these simulations, every node, actually, represents the transceiver for an apartment that sends and receives the required information and data about it. A ZigBee end device could not cover the desired range for this purpose. The time per simulation in these cases was 20 minutes.

In Both Area Networks we were interested to examine how our configuration would affect the following parameters:

- End to End delay: It refers to the time taken by the packets to be transmitted from the source node to their destination including all the delays that may happen during route discovery latency, retransmissions delays at the MAC layer, propagation and transfer times. The higher the end to end delay is, the poorer the performance of the existing configuration is due to network congestion.
- Throughput: The ratio of the total amount of data that is received by node from the source to the time that it receives the last packet. It has an inverse relation with the delay in a network.
- Number of hops per route: Each packet, according to the availability of their neighbors and according to the protocol that is implemented, follows a specific

route to reach its destination. The hops correspond to the number of the nodes that a packet included in its route to be delivered successfully

4.1 Networking issues within a Home Area Network

Building a Home Area Network using Opnet we have chosen an area of 100m^2(10x10meters) to simulate our experiments. Below, all the scenarios that were tested are available, containing all the possible combinations of the described parameters. Moreover, we tried to verify how the network reacts in a different number of included devices.

Specifically, in the following scenarios we will present the way our network has been affected by different values of:

Data rate
Bandwidth
Topology
Coordinator location
Number of hops

Table 4.2: HAN scenarios parameters

Moreover in the following scenarios are included the following devices:

ZigBee	Coordinator
ZigBee	Router
ZigBee	End Device

Table4.3: HAN devices

4.1.1 Scenario 1

As it is mentioned in 3.3 the ZigBee protocol has a limit in its data rate the 20Kbps. The simulations that have been run used as data rate that limit of 20Kbps and the amount of 100Kbps.

However, we wanted to check protocol's limits trying to find out how a network would react if every device has been configured to transmit and receive in 500bps. Our perspective has more or less the results that we expected.

The following parameters have been set:

PARAMETERS	VALUES
Bandwidth	400KHz for every device
Data Rate	500bps
Frequency	868MHz
Algorithm	CSMA/CA
Topology	Hierarchical Tree
Position of nodes	Randomly
Devices	1 Coordinator, 4 routers, 16 end devices

Table 4.4: Scenario 1 parameters

Specifically, regardless of how the rest parameters were defined, our simulations with the particular data rate conclude to a failure of the network that is depicted on Figure 4.3. Actually, from the beginning of the simulation there is no traffic generated and since 720sec of simulation have been completed a linearly increase in the end to end delay is noticed until the end of simulation. Obviously this data rate applied to the devices cannot be supported by the network and ZigBee protocol.

This is enhanced even more by the number of hops. As it is depicted in Figure 4.2, there is only one hop has taken place until the end of the simulation. This is the messages that have been sent by the Coordinator to the routers to explore the topology of the network. None of the rest devices during the total simulation has sent any data. That is why the throughput corresponds to such low levels, Figure 4.4.

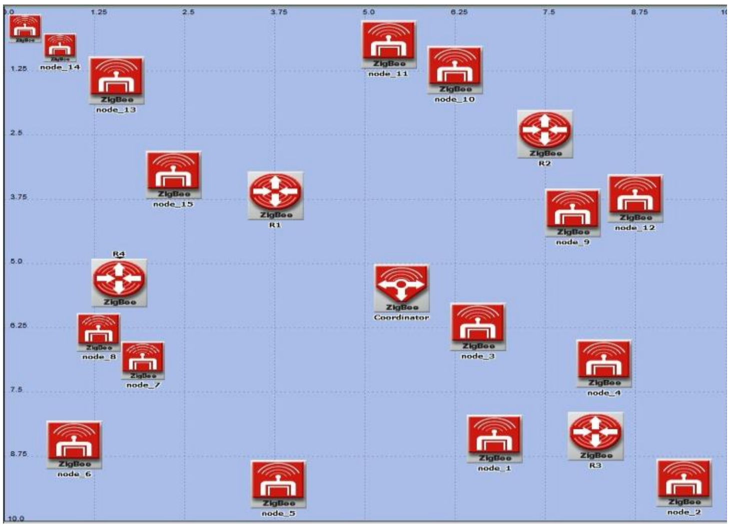


Figure 4.1: ZigBee Network in a random topology

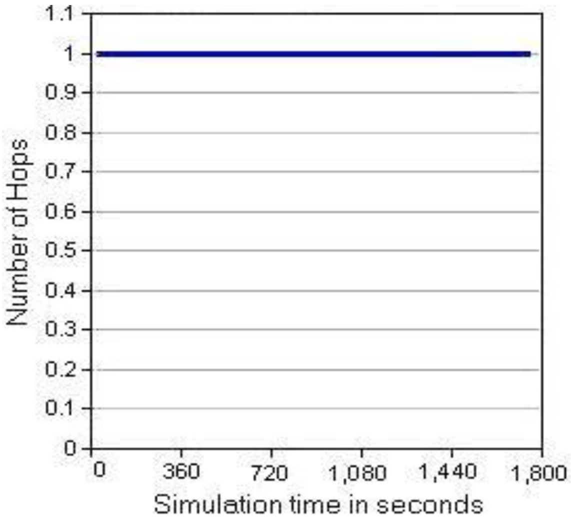


Figure 4.2: Number of hops

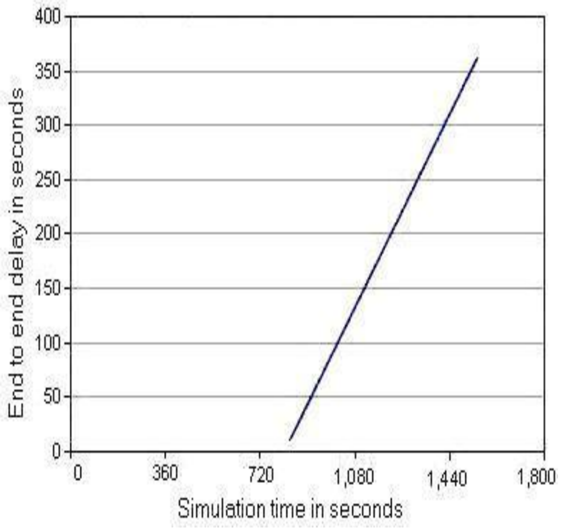


Figure 4.3: End to End Delay

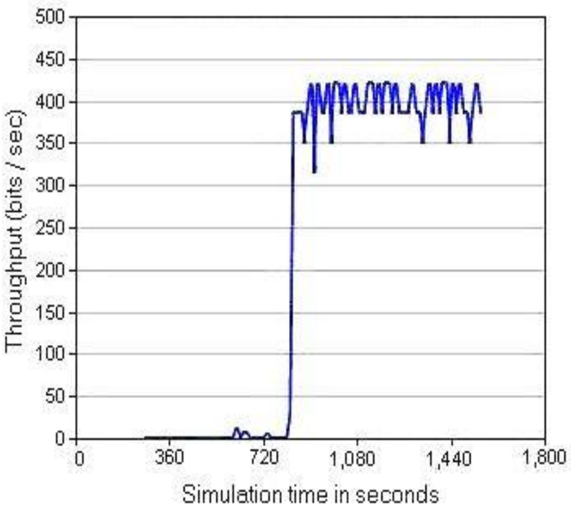


Figure 4.4: Throughput

4.1.2 Scenario 2

Let’s examine now the differences that occur concerning two valid values for the data rate. Consequently we configured our network of Figure 4.1, to a data rate of 20Kbps and 100 Kbps. We tested these two rates in a random structure implementing a Hierarchical topology.

The following parameters have been set:

PARAMETERS	VALUES
Bandwidth	400KHz for every device
Data Rate	20Kbps and 100Kbps
Frequency	868MHz
Algorithm	CSMA/CA
Topology	Hierarchical Tree
Position of nodes	Randomly
Devices	1 Coordinator, 4 routers, 16 end devices

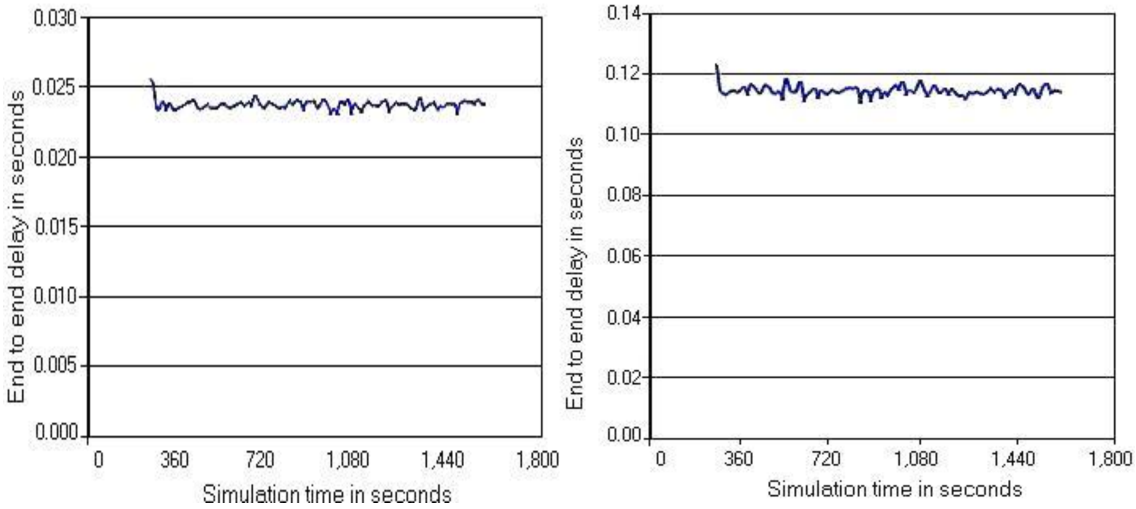
Table 4.5: Scenario 2 parameters

When we have set as data rate the 20Kbps to the devices we can see that there is a satisfying end to end delay to the network along the total time of the simulation. As it is shown in Figure 4.5(a), the packets are traversing across the network without any problem since the end to end delay is about 0.022secs. Of course this kind of delay is the expected one because we should not forget that the main characteristic of ZigBee protocol is that it allows communication in a low data rate. Moreover, the frequency we investigate is the ideal for this particular data rate.

On the other hand, when we implement a data rate of 100Kbps there is a significant difference on the network's operation. There is an accepted delay of 0.11secs for a packet to be delivered successfully to the destination. Furthermore, this time the end to end delay has also that particular value during the total time of the simulation, Figure 4.5(b), even though tat data rate is can be supported in another transmission band in a better way.

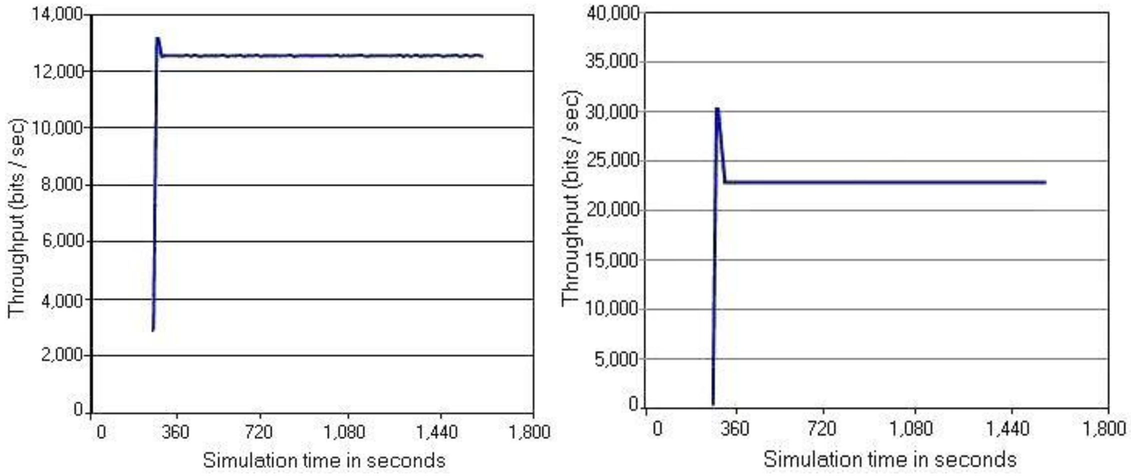
In Figure 4.6, we can see that there is more throughput in the 100Kbps as it was expected than in the 20Kbps. Actually, there is an increase of almost 50%. But the interesting point in these simulations is the following, Figure 4.7. There is not a heavy difference as far as the number of hops is concerned across the network. In both data rates there is a great stability concerning the routing and the forwarding of the packets since they adopt totally the Hierarchical topology. As you can see there are exclusively two hops, from end devices to routers and from there to the coordinator.

Therefore, there is greater amount of data, larger delay for this data to be delivered but the route does not change at all. The devices sensing that the channel is free and the router is idle then they are able to transmit their data to it. The routers act in a similar manner to contact the Coordinator operating in the adapted topology. It is very encouraging though, that even with this increment in the data rate the network is able to tolerate and serve its nodes and their traffic successfully.



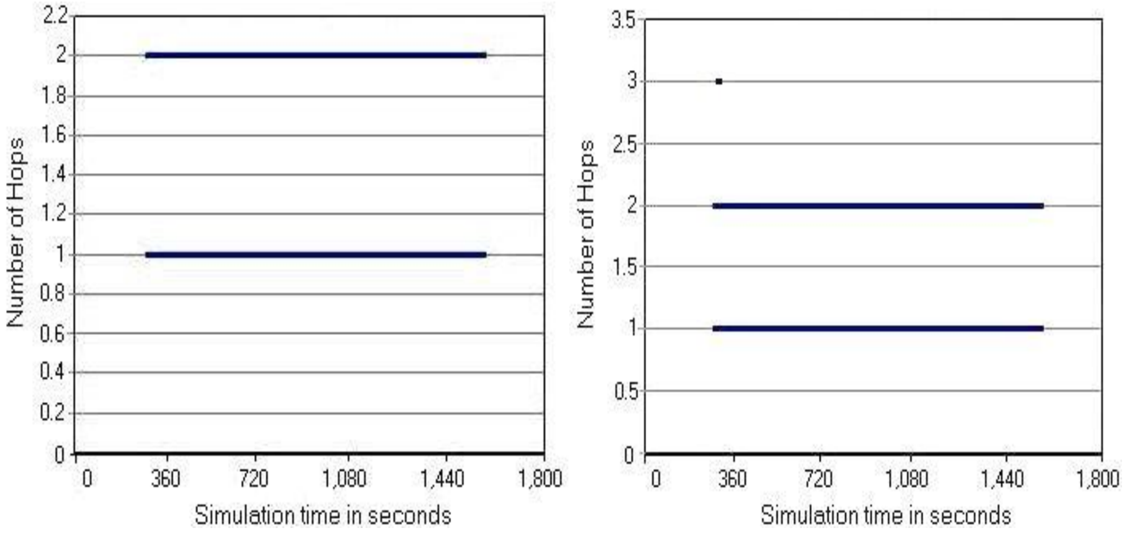
(a) (b)

Figure 4.5: End to End Delay for a) 20Kbps and b) 100Kbps



(a) (b)

Figure 4.6: Throughput for a) 20Kbps and b) 100Kbps



(a) (b)

Figure 4.7: Number of hops for a) 20Kbps and b) 100Kbps

4.1.3 Scenario 3

This scenario has the perspective to evaluate how the bandwidth can differentiate the network's attitude. We set as data rate the most efficient from the previous simulations which as it was proven is the 20Kbps.

The following parameters have been set:

PARAMETERS	VALUES
Bandwidth	70KHz, 270KHz and 400KHz for every device
Data Rate	20Kbps
Frequency	868MHz
Algorithm	CSMA/CA
Topology	Hierarchical Tree
Position of nodes	Randomly
Devices	1 Coordinator, 4 routers, 16 end devices

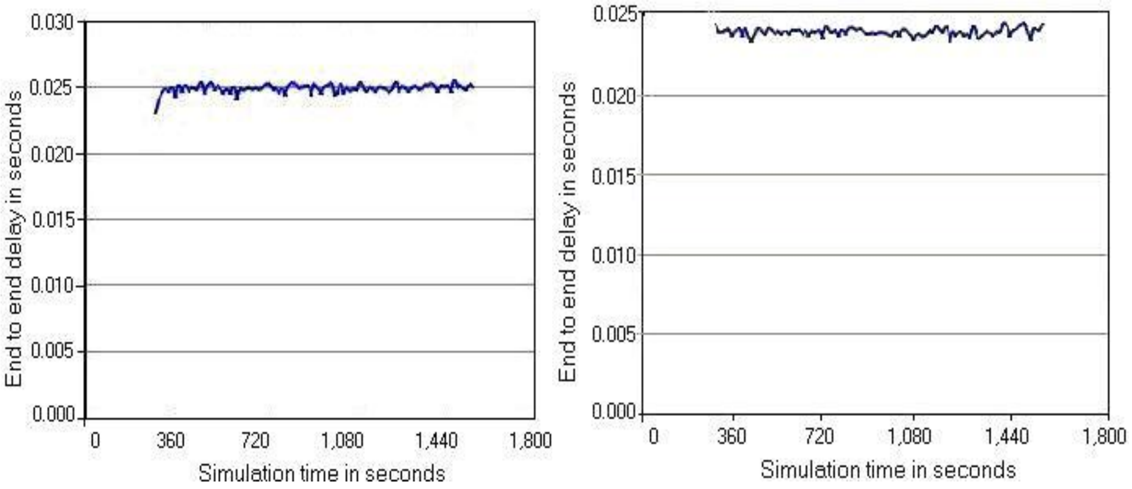
Table 4.6: Scenario 3 parameters

The results using as bandwidth 400 KHz are available in the previous scenario with 20Kbps. When the bandwidth increases there is better stability as far as the routing across the network is concerned. Consequently, that means that the generated traffic can be managed in a more efficient manner than it could be in a lower bandwidth. Our expectations for that scenario were as we configure our simulations in a higher bandwidth we have to wait lower end to end delay and fewer hops, as well.

As we can see in Figure 4.8, that was totally true since in a 70 KHz bandwidth we have 0.025 sec end to end delay, which becomes 0.024 sec in a bandwidth of 270 KHz and it is even lower, approximately 0.023 sec, when we apply 400 KHz as bandwidth, Figure 4.5 (a).

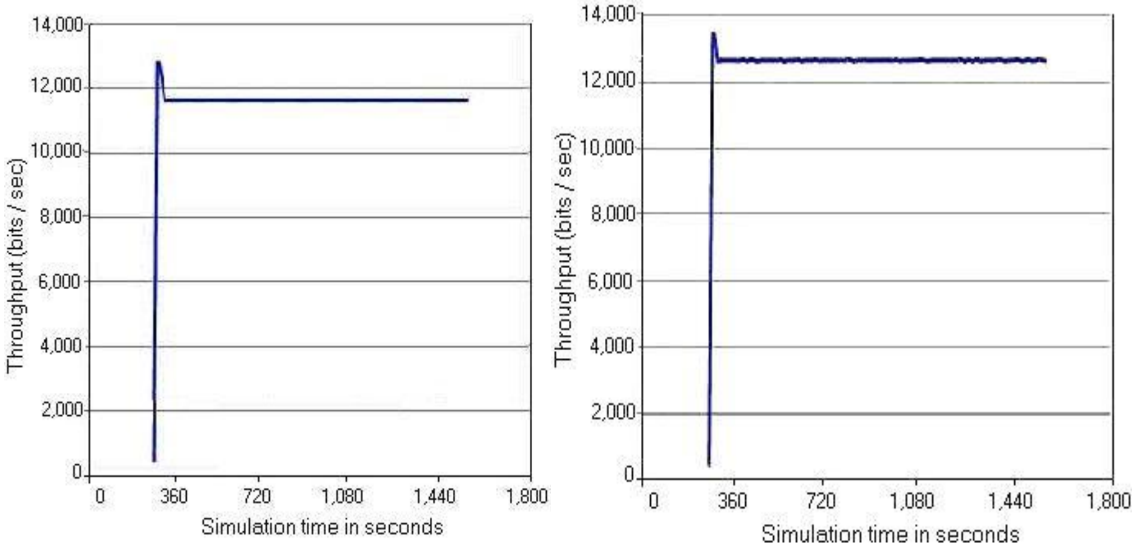
Concerning the throughput, there is also a slight increment as we increase the bandwidth. Actually, from 11,700 bits per sec in 70 KHz we get a throughput of 12,800 bits per sec increasing the bandwidth to 270 KHz, Figure 4.9.

Finally, concerning the routing we did not meet our expectations in this sector. Specifically, we expected lower hops in higher bandwidth but in all the cases there is a very stable routing across the network. The strange is that in higher bandwidths it is noticed that a 3rd hop was needed in the beginning while at 70 KHz we have strictly 2 hops. Except for that, the number of hops had no alteration, Figure 4.10, and that is probably owed to the small change of the end to end delay. Particularly, delay and routing have an inverse relation with each other, meaning that when the delay is reduced the routing should be more stable which did not happened in our simulation.



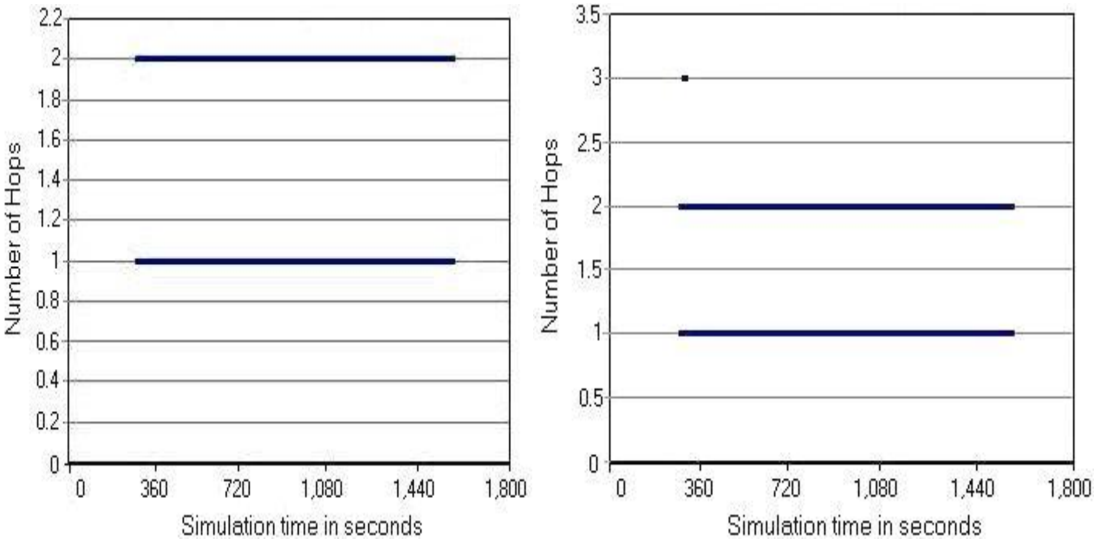
(a) (b)

Figure 4.8: End to End Delay for a) 70KHz and b) 270KHz



(a) (b)

Figure 4.9: Throughput for a) 70KHz and b) 270KHz



(a) (b)

Figure 4.10: Number of Hops for a) 70KHz and b) 270KHz

In other words, the results we extracted by our experiments are totally applicable to the theoretical expectations we had. It is absolutely logical for a network increasing the bandwidth to decrease the end to end delay. That is happening since the bandwidth for a network is the provided speed that the data can be transmitted. Therefore, a packet needs less time to reach the same destination than the respected time with a lower bandwidth.

With regard to this, we could assume that a lower delay means fewer hops in the packet's route. That is absolutely justified since when a packet visits many nodes (hops) until getting to its destination it has greater delay. Consequently, we supposed that this would happen in our experiments, too.

However, we did not consider the network's topology, the number of sub-networks and the number of end devices. Particularly, there are four sub-networks with four devices each one, operating in a hierarchical structure. This total structure could not have great differences concerning the number of hops. In case we had more devices or a star topology or a fully mesh topology maybe there would be differences in this aspect, too. Such scenarios are available below as you will see.

Finally, as far as the throughput is concerned there is an analogous relationship between it and the bandwidth. That is explained by the Shannon-Hartley theorem:

$$\boxed{C = B\log_2 \left(1 + S/N\right)}$$

where we can see that the channel capacity (which is the achievable throughput) can be affected by the bandwidth and the signal to noise ratio.

Consequently, in the following scenarios we had chosen obviously to use as parameters the ones that are most efficient so far. That is the reason we configured the rest simulations with a bandwidth of 400 KHz and a data rate of 20Kbps.

4.1.4 Scenario 4

This particular scenario takes under consideration the position of the nodes. Specifically, we built a topology in a Manhattan structure where every device has a same distance from its parent router with the rest ones, Figure 4.11.

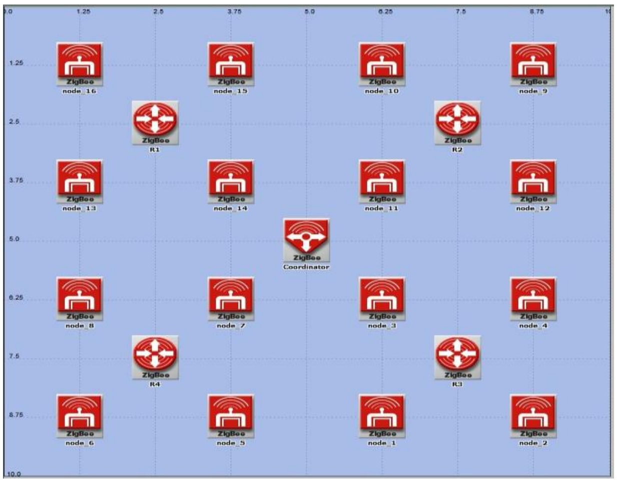


Figure 4.11: Network in a Manhattan structure

Therefore, under these circumstances we guarantee that no end device would need more than two hops to send its data to the destination, since every device reaches directly its parent router. This is actually what is happening as we can see in Figure 4.12.

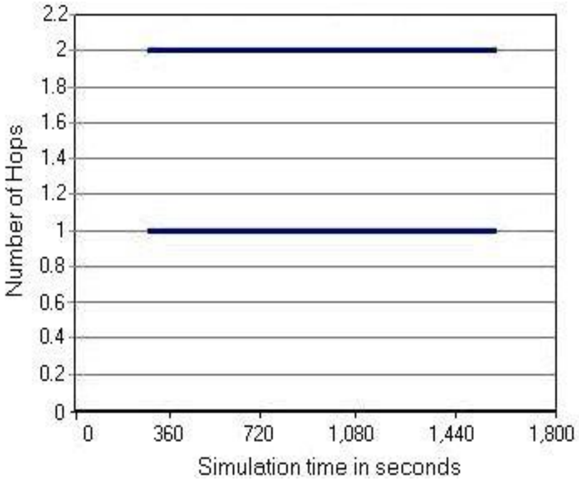


Figure 4.12: Number of Hops

Moreover, when the nodes are located randomly, we investigated how the Coordinator's position could affect their operation. Consequently, we placed it in a non central position to see how the remote nodes and routers would correspond in conjunction with the rest network so that it can be efficient.

The following parameters have been set:

PARAMETERS	VALUES
Bandwidth	400KHz for every device
Data Rate	20Kbps
Frequency	868MHz
Algorithm	CSMA/CA
Topology	Hierarchical Tree
Position of nodes	Randomly and in a Manhattan structure
Devices	1 Coordinator (centrally located and non centrally located), 5 routers, 15 end devices

Table 4.7: Scenario 4 parameters

In a Manhattan structure in conjunction with the specific environment size of our experiments and the number of included end devices we did not expect to see great differences in the network's attitude. That is because 16 end devices and 4 routers are more than capable to cover that environment. Especially when their function is defined to be in a Hierarchical topology where the devices belong to separate sub networks there are no so many possibilities great abnormalities to be noticed from the random structure we had created to a Manhattan one. The graphs below verify our expectations since we notice that there is a slight reduce in both end to end delay and throughput.

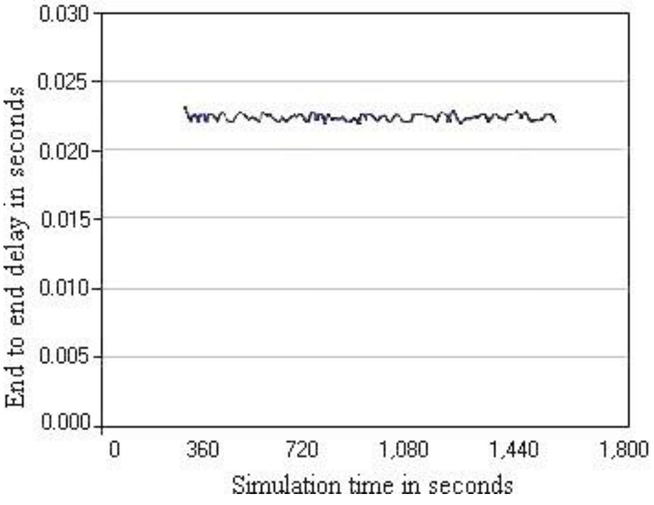


Figure 4.13: End to End Delay

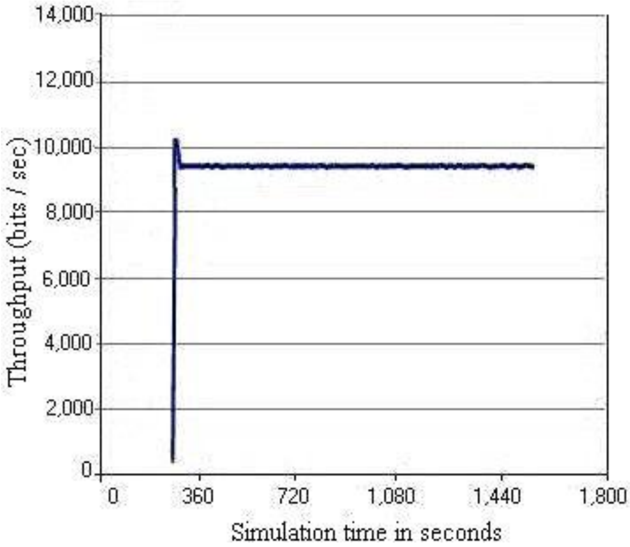


Figure 4.14: Throughput

Concerning the position of the coordinator, we had similar results when we tried to change its central position. As it is mentioned and above in details we did not expect great alterations in our results, given the particular random structure that we simulated.

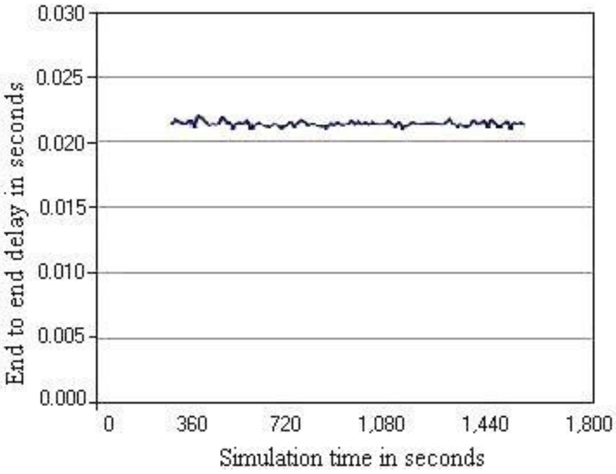


Figure 4.15: End to End Delay for a non Central located Coordinator

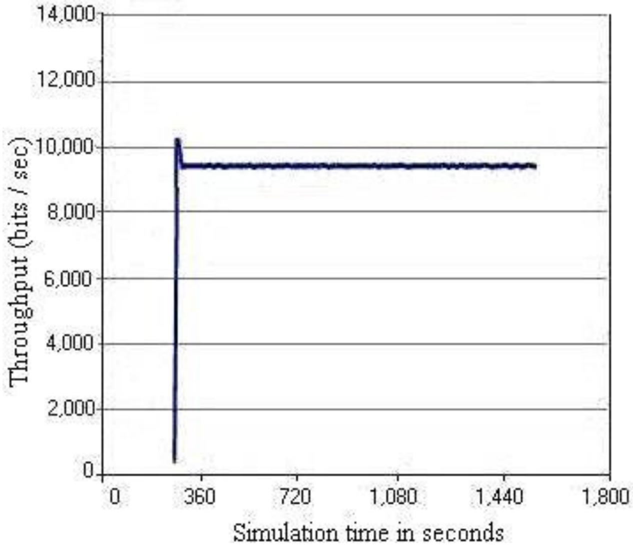


Figure 4.16: Throughput for a non Central located Coordinator

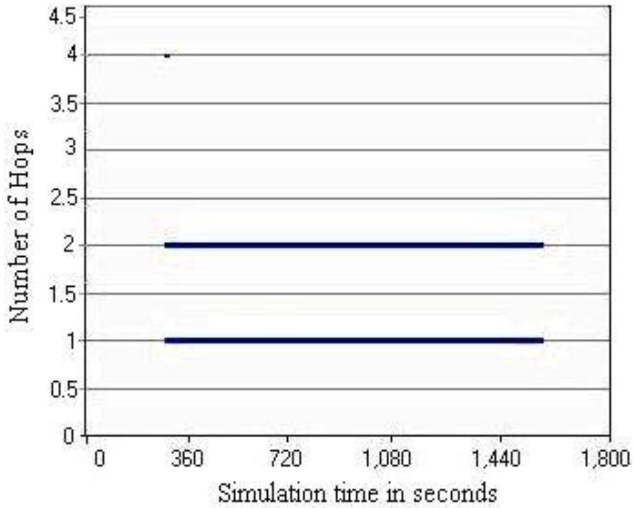


Figure 4.17: Number of Hops for a non Central located Coordinator

4.1.5 Scenario 5

In all the previous simulations we had defined as a topology the Hierarchical topology, where the Coordinator (root) receives from the routers and the routers receive from the nodes.

This scenario identifies the how network of Figure 4.1 reacts when implementing a fully mesh topology in the network.

The following parameters have been set:

PARAMETERS	VALUES
Bandwidth	400KHz for every device

Data Rate	20Kbps
Frequency	868MHz
Algorithm	CSMA/CA
Topology	Fully Mesh
Position of nodes	Randomly
Devices	1 Coordinator, 4 routers, 16 end devices

Table 4.8: Scenario 5 parameters

Obviously, in that way it is expected an increment in all the three attributes to take place. That is because, the routers are not able anymore to control the generated traffic but only facilitating it, by participating in the routes of the packets.

Actually, as we can see and below in the results, there was an increase, not a heavy one hopefully, to the end to end delay from 0.023 to 0.029 seconds.

The same it is for the throughput which is now at 27.000 bits per second from 23.000

And for the number of hops which are now at least three per route while they reach up to nine in the beginning of simulation.

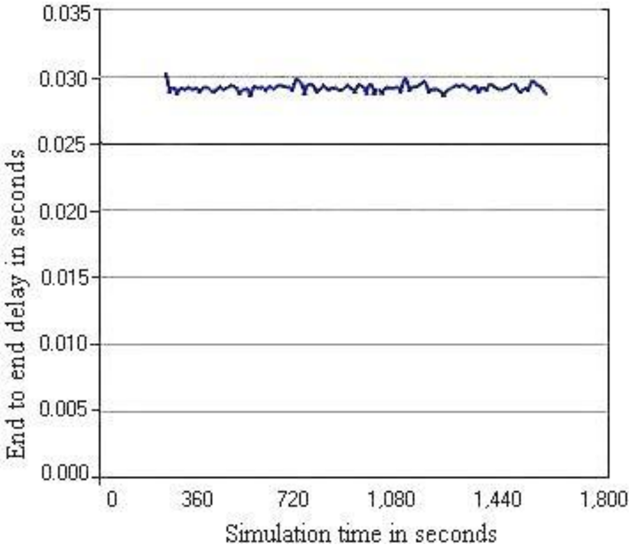


Figure 4.18: End to end delay

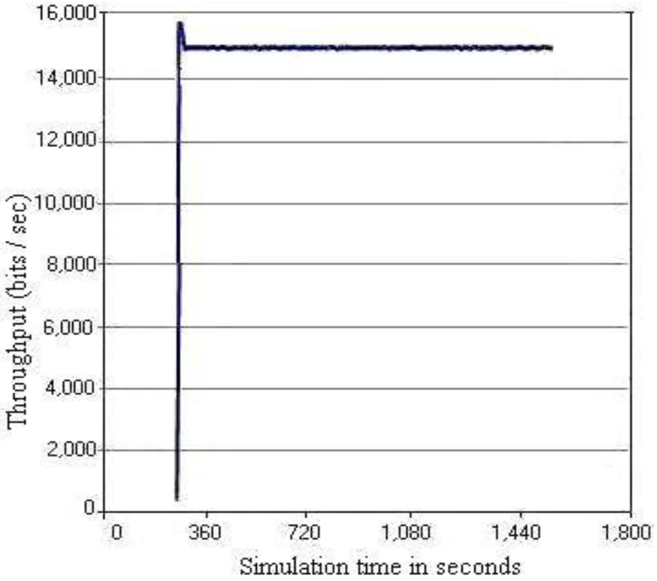


Figure 4.19: Throughput

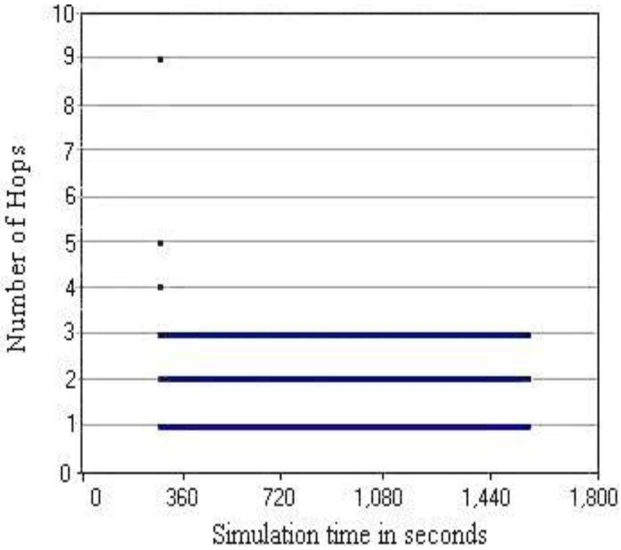


Figure 4.20: Number of Hops for a non Central located Coordinator

Those results are absolutely logical because at first there is absence of the hierarchical structure. Therefore, the nodes forward their packets not only to routers but in every single device that is idle and inside their range that particular moment. That device could be either another end device or a router or even the coordinator. In that way there is the opportunity for a device to send directly its data to the coordinator but the possibilities are small since 16 devices have that opportunity.

4.1.6 Scenario 6

In this particular scenario we intend to check out the network's tolerance by increasing the existing end devices to 48, without changing anything as far as the routers and coordinators are concerned, figure 4.21. We simulated for hierarchical and fully mesh topology as well.

The following parameters have been set:

PARAMETERS	VALUES
Bandwidth	400KHz for every device
Data Rate	20Kbps
Frequency	868MHz
Algorithm	CSMA/CA
Topology	Fully Mesh, Hierarchical Tree topology
Position of nodes	Randomly
Devices	1 Coordinator, 4 routers, 48 end devices

Table 4.9: Scenario 6 parameters

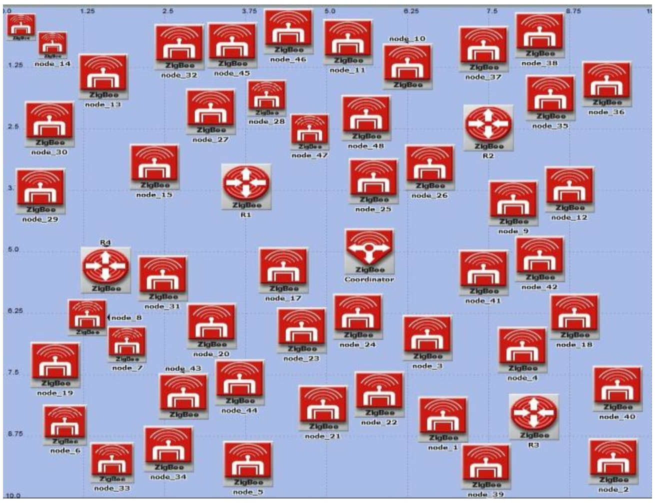
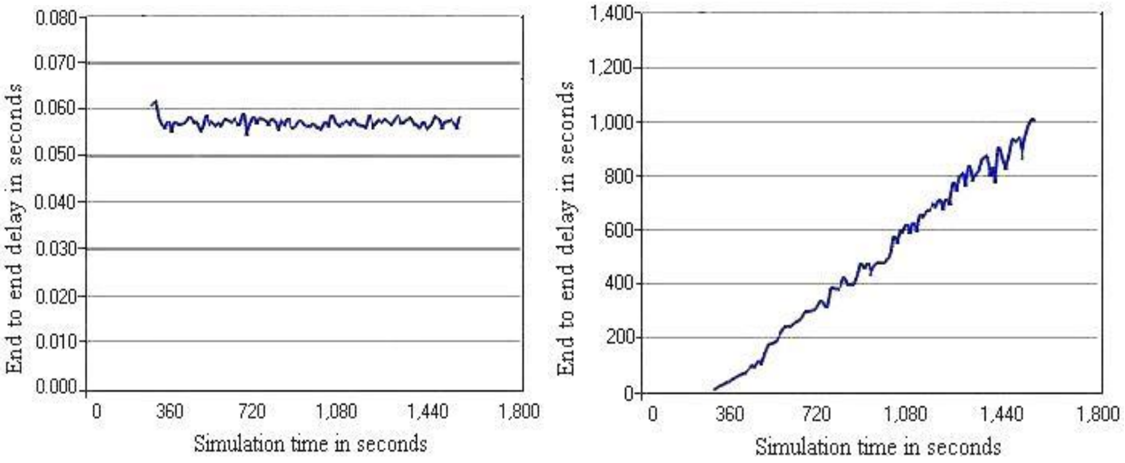


Figure 4.21: HAN with 48 end devices

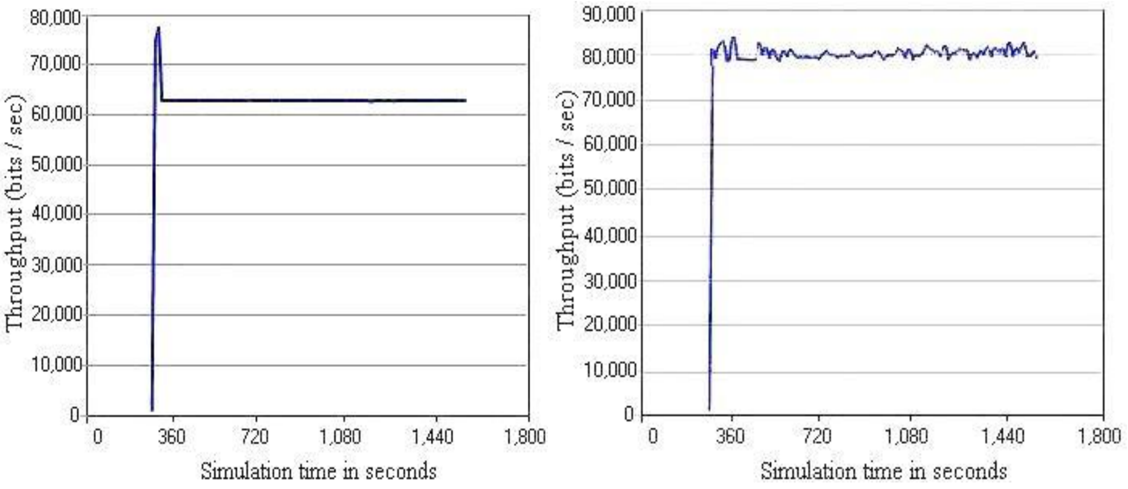
When we have for the same network three times more the nodes that we have before, we expect the network to reach its limits. Particularly, the specific network seems to correspond very efficiently when a Hierarchical topology is set.

However, it fails when we implement a fully mesh topology. Although there is not a mass increase on the throughput, the network is not able to tolerate so much uncontrolled generated traffic within it. The massive hoping that takes place across the network in coordination with the great amount of data that cannot reach their destination, creating an infinite end to end delay, lead to the disoperation of the network. We astonishingly see that end to end delay reaches up to 1,000 seconds which means that a packet wants almost 16 minutes to get to its destination which makes the network fails.



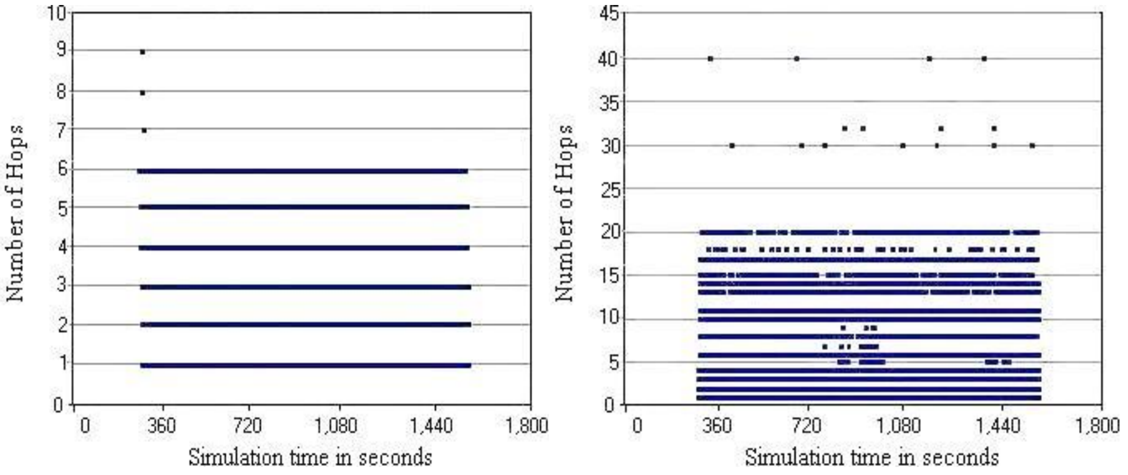
(a) (b)

Figure 4.22: End to end delay for a) hierarchical and b) Fully Mesh



(a) (b)

Figure 4.23: Throughput for a) hierarchical and b) Fully Mesh



(a) (b)

Figure 4.24: Number of hops for a) hierarchical and b) Fully Mesh

That massive hopping is happening due to 2 reasons. First of all, there is not the order of a hierarchical structure which also divides the network in stages making easier its operation. Consequently, having the freedom every transmitter to send the packets to every idle node there is great possibility as it is depicted above for the packets to have a long travel until reaching their destination. Hypothetically, if we had increased even more the data rate we may have a total flooding over the network ending up with a total failure in the beginning.

What is more, we increased the number of included nodes which has a dual role concerning the services of the network. When a node wants to transmit has a flexible route to select but also there is great possibility with a large data rate a packet to include many hops in its route to get to its destination.

4.2 Networking issues within Neighborhood Area Network

This particular task has been developed focused on the same parameters as its basis. Specifically, we wanted to examine what is a neighborhood area network's attitude according to the data rate and bandwidth of its nodes. In addition, we ran simulations to compare the results that we would extract according to the position of the nodes; randomly or in a Manhattan structure.

However, there are some parameters that we had to check in a different point of view. Particularly, it is very important to understand how we would configure our topology concerning the distance of the nodes which is a factor of great importance for these networks. Below, the presented scenarios test how the generated traffic and the network's operation differ in a distance of 25 and 50 meters among the devices. In that way, combining different number of included nodes we were able to check the tolerance of the network according to its density and its scale.

Initially when we tried to run a simple simulation on Opnet modeler with a few devices to test our configuration we noted that the range of a single device was very wide almost at 2 kilometers. To reduce that range we had to change their receiver's antenna sensitivity from 95dBm to 76dBm and their transmission power from 0.005W to 0.001W.

Finally, we implemented two ad-hoc routing protocols to understand how every one of them could affect the specific topologies and their efficiency.

In detail, the configuration of these simulations was the following:

PARAMETERS	VALUES
Bandwidth	70KHz, 270KHz and 400kHz for every device
Data Rate	1Mbps and11Mbps
Frequency	800MHz
Algorithm	IP
Topology	Fully Mesh
Position of nodes	Randomly and in a Manhattan structure
Ad hoc routing protocols	1. AODV 2. OLSR

Table 4.10: NAN scenarios parameters

In all the simulations we used fixed wireless nodes and server having an environment size of 0.25km^2 (500X500 m), using as an application FTP. Their operation mode is set to be serial and random. The simulation that was used is DPSK. The scenarios were simulated for 1800sec.

4.2.1 Scenario 1

Initially we will present the attitude of the network when it includes ten, twenty, forty nine and one hundred twenty two nodes. Implementing AODV as routing protocol, we will discuss the differences that are noticed in throughput, delay and hopping across our network concerning the size of the network.

Network1

There are ten nodes located in a Manhattan structure as it is shown in Figure 4.25, around the Server which is in the middle of our topology.

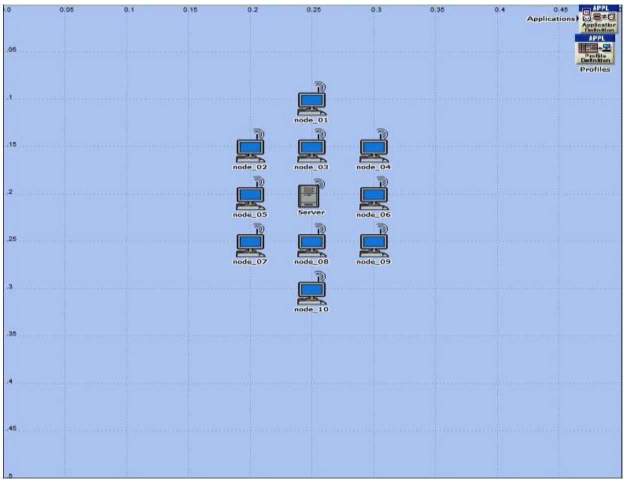


Figure 4.25: NAN of ten nodes

Running the simulations we focus on characteristics, hops per route, end to end delay and throughput.

First of all, we wanted to examine how many hops per route would happen in average during the simulation. As it is shown, there are no great demands in this sector, while during the total simulation the nodes for a route do not include more than 3 hops for the packet to be delivered successfully, as it is shown in Figure 4.26. This is absolutely normal since for the nodes that are not neighbors with the server we expect to use their neighbors as intermediate nodes to deliver their data.

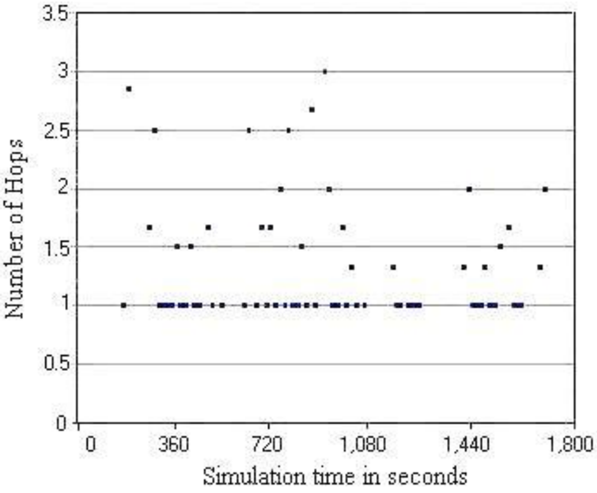


Figure 4.26: Number of Hops per route

Consequently, since the network seems to be able to serve the sessions that are created, we could not expect an essential delay to occur and the result verifies our expectations. As it is depicted in the Figure 4.27 there is a delay of 0.009 seconds across the simulation time which means that in average the time taken by a packet to be transmitted from the source to destination was about 0.0008-0.00085 sec.

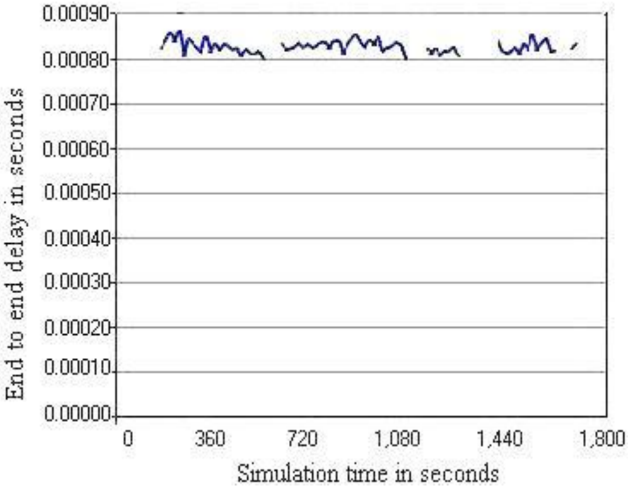


Figure 4.27: End to end delay

Moreover, a low delay means that there will be a high throughput. Throughput is the ratio of the total amount of data that a receiver receives from a sender to a time it takes for the receiver to get the last packet. As we can see in Figure 4.27, there is a throughput up to 14.000 bits per sec. In the beginning throughput reaches up to the peak of 25.000 bits since AODV causes the flooding until the route tables to be constructed.

Finally, we noticed that there are some periods that no traffic is generated at all. That occurs since we have defined our nodes to sent serial but randomly (and not ordered) their data and in combination with the limited population of nodes it is logical such periods to exist during the simulation. Consequently, those particular moments the nodes of the network do not transmit but in the following networks there are not such time slots where nobody wants to transmit.

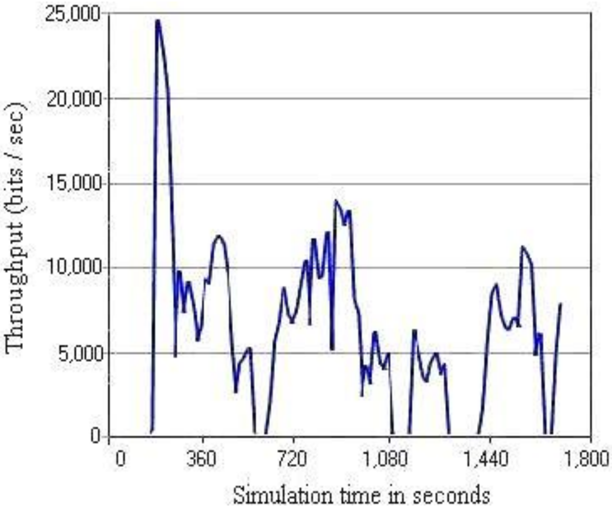


Figure 4.27: Throughput

Network 2

In this case we doubled the existing nodes without changing anything else in the structure and the operation of the network. Our perspective is to find out in which way the same specific characteristics alternate. The new network is shown in Figure 4.28.

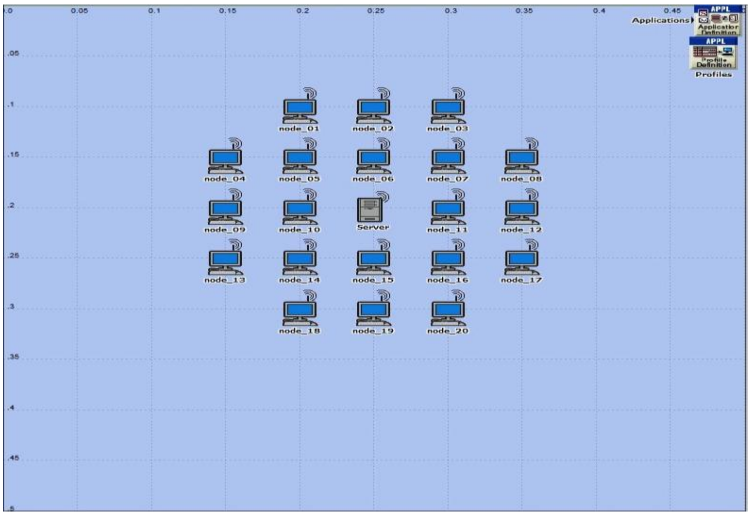


Figure 4.28: NAN of twenty nodes

As far as the hopping is concerned we can see that there is a slight increase in the average number of hops per route during the simulation, since there are more routes that need 3 hops to deliver their packet than before but we cannot say that there is a great effect on the hopping by increasing the number of nodes up to twenty.

Besides, that not so important difference in the network’s operation is depicted by the end to end delay. In the Figure 4.29, we can see that the delay remains almost the same as in the previous simulation.

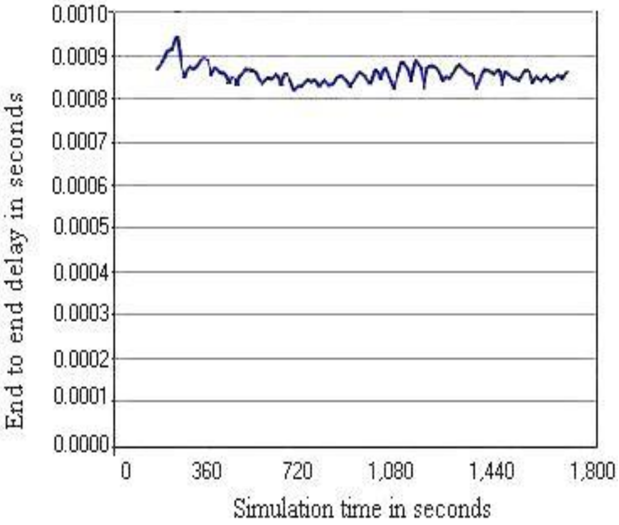


Figure 4.29: End to end delay

The interesting fact of this experiment has to do with the throughput. It would be absolutely normal to expect that since delay and number hops per route did not have an important change the same would happen with the throughput, as well. However, that could not stand because we doubled our nodes therefore we increased the generated traffic in the network which causes the throughput that is shown in the Figure 4.30.

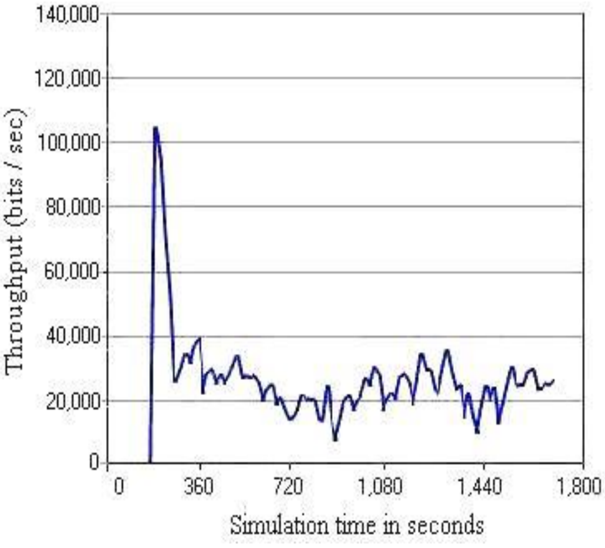


Figure 4.30: Throughput

Network 3

The previous topology seems not to affect much the network's operation even if we increased one hundred per cent our initials nodes.

Our curiosity could not stop there. Thus, we try to test our network's attitude even more, locating this time 48 nodes around the server, Figure 4.40.

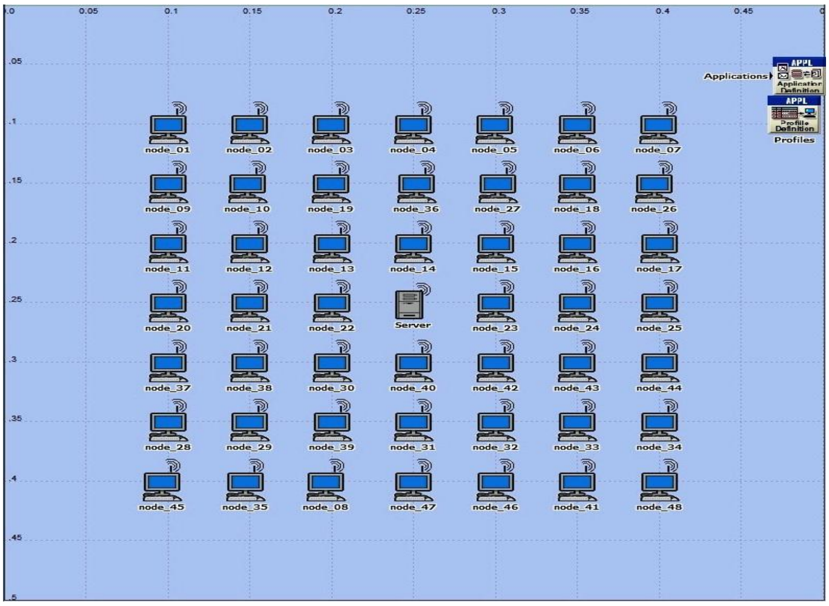


Figure 4.40: NAN with 49 nodes in a Manhattan structure

The average number of hops per route in the network has even now a very slight difference according to the previous ones.

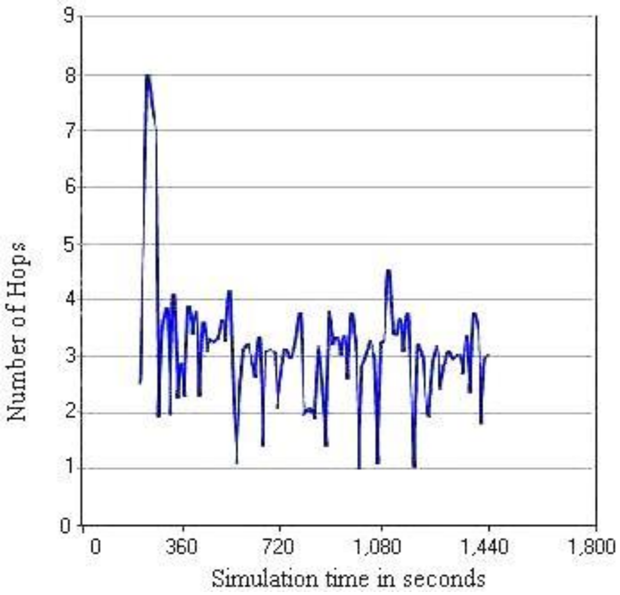


Figure 4.41: Number of hops per route

But in this topology we have noticed that the remote nodes of our topology require a great number of hops for their routes which did not happened before. The nodes that had the largest distance from the server needed sometimes up to 4 or 5 hops per route. In this network these nodes demand up to 9 hops for some routes to deliver their packets. Consequently, even if the average number of hops per route does not increase essentially there are great differences. The fact that the average number has no important fluctuations is because the neighboring nodes to the server demand one or two hops per route giving a result that actually could mislead our investigation about the routing operation and efficiency.

Nevertheless, we notice that the delay in the network does remain in the same low levels, which is really satisfying, but there is an expected increase since we add many more nodes than before, Figure 4.42.

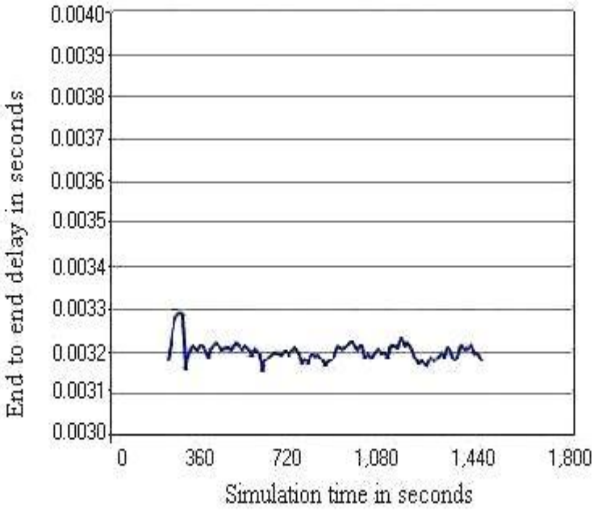


Figure 4.42: End to end delay

Additionally, the throughput has overcome the 100,000 bits per sec, Figure 4.43. Even with that particular throughput the network could respond to the high load without failures.

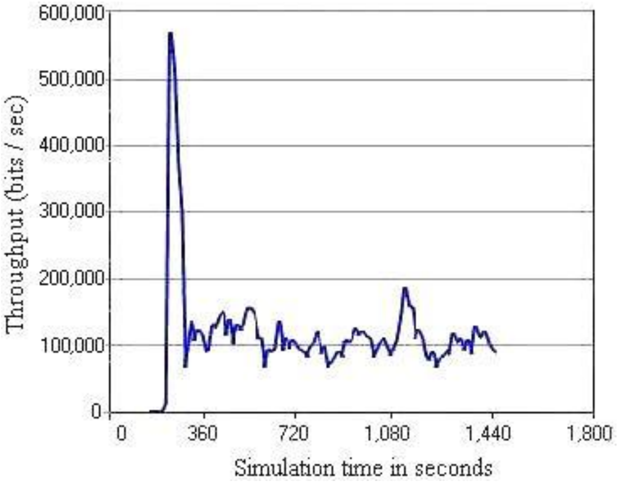


Figure 4.43: Throughput

Network 4

By increasing the number of nodes we realized that our network is able to serve the sections that are generated across it.

By this particular simulation we wanted to investigate how the increase of the nodes but also the increase of the density in the network could affect our topology, Figure 4.44.

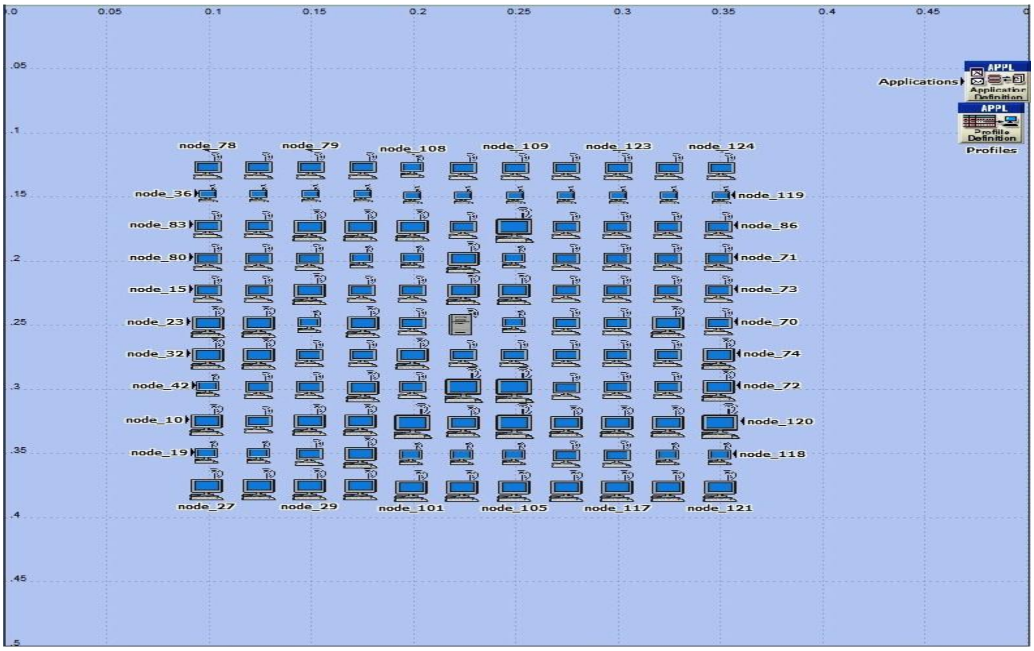


Figure 4.44: NAN with 122 nodes in a Manhattan structure

Specifically, we increased the nodes to 122, but this time every node is at 25 meters from its neighbor. That is actually means that we have almost 3 times more nodes than in the previous network inside an area of 250X250meters instead of 300X300meters.

The number of hops per route has been increased in the following way. We can see that this topology demands more often the included routes to be accomplished with 3 nodes per route in average, Figure 4.45.

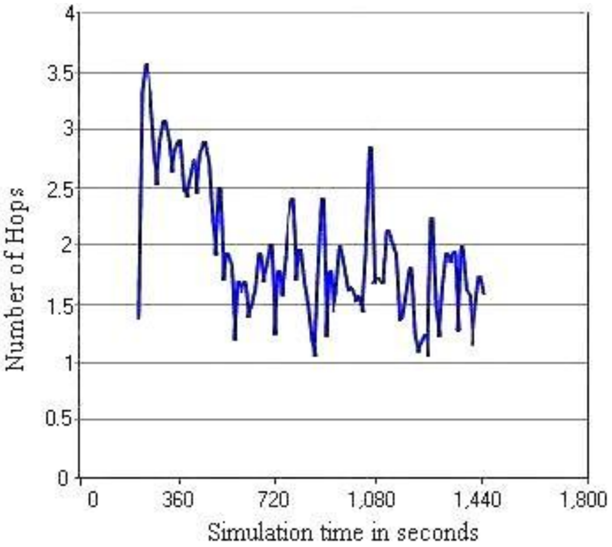


Figure 4.45: Number of hops per route

In this scenario we did not change the range per hop so even a node that has 2 nodes between it and the server is able to send its data directly to the server even by one hop. Due to the density of the network some of these nodes during the simulation need three nodes per route but that is something that is happening occasionally. The nodes that are at the edges of the network need up to 4 hops per route to deliver their packets when in the previous simulation such nodes required up to 9 hops for some routes for successful transmission. In case we reduce their sensitivity we would have very different results but this is not in the scope of our investigation.

Furthermore, the delay for this topology has been increased even more than before at 0.006 sec, which is absolutely logical according to the details we have just mentioned and the number of the included nodes, Figure 4.46.

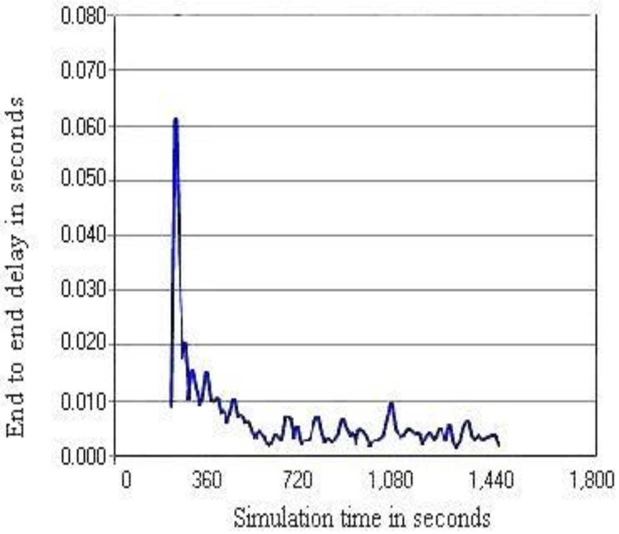


Figure 4.46: End to end delay

As for the throughput of the network, it reaches up to 6.500.000 bits/sec, having as mean the 1.000.000 bits/sec.

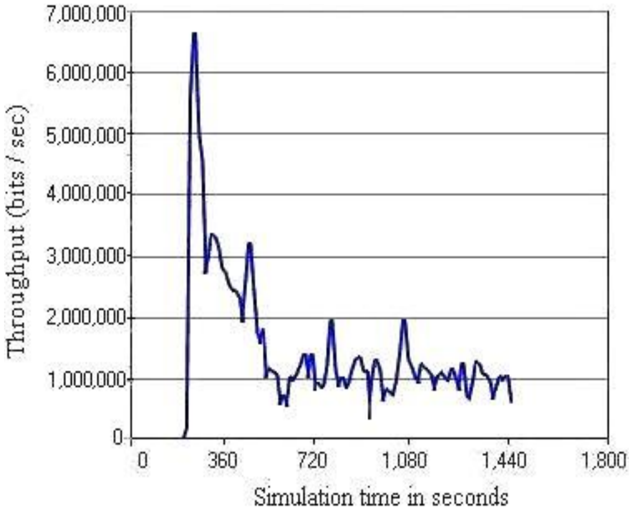


Figure 4.47: Throughput

4.2.2 Scenario 2

In this particular scenario we have chosen as a default network the one with the 49 nodes to test it by configuring the data rate.

As far as the Network 3 (Figure 4.40) is concerned when we increase the data rate we expect to have an increase in all the three parameters that we investigate. Logically since we increase the amount of the information that traverses the network without configuring anything else like bandwidth for example, we would not expect less throughput and less delay. Especially in a network like that one where all the apartments (nodes) communicate among them trying to deliver their data to the central server. That means that with more bits of data there are no routers to facilitate the generated traffic keeping the investigated parameters at the same levels. The results we extract from the simulations attached exactly to our predictions as you can see below.

Nevertheless, the network tolerated to the new data rate which is eleven times greater without any failure until the end of the simulation

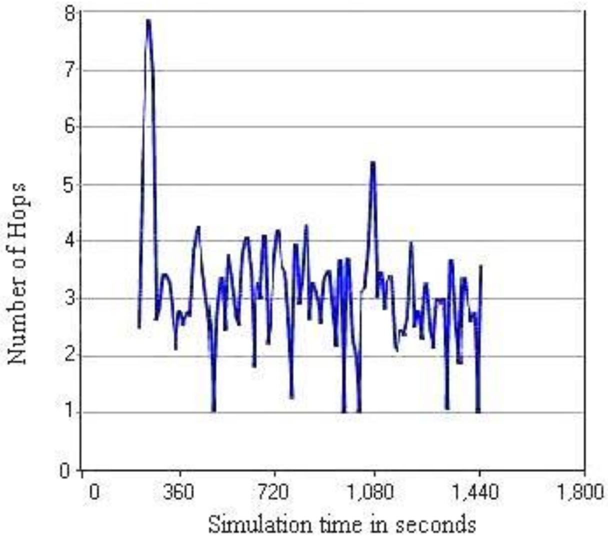


Figure 4.48: Number of hops per route

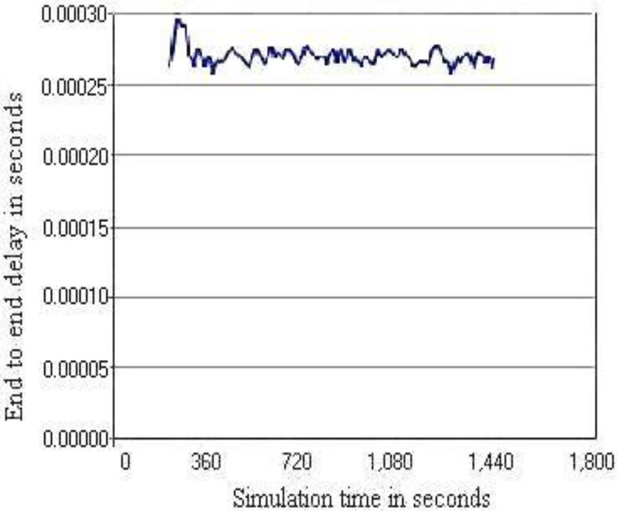


Figure 4.49: end to end delay

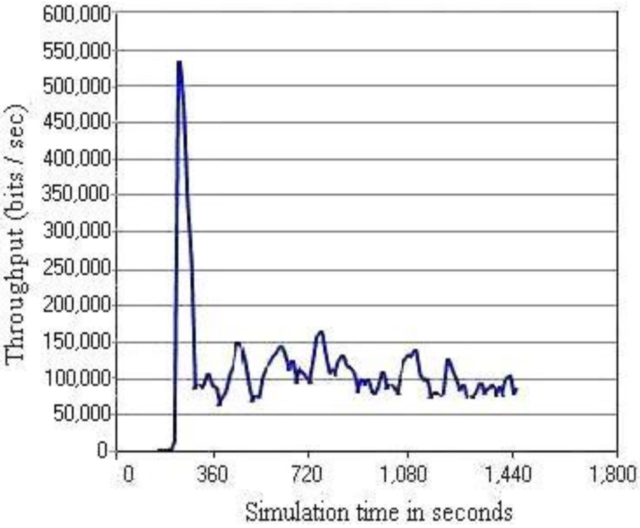


Figure 4.50: Throughput

However what is going to happen if we implement these different data rates to a random topology. Could all the nodes of the topology correspond to these changes? Would that network have the same tolerance as the one the previous network had?

To examine that, we built the following network with the same number of nodes. However, there is not the facility of the specific distance as before in order for every node to be able via an intermediate to transmit its data successfully.

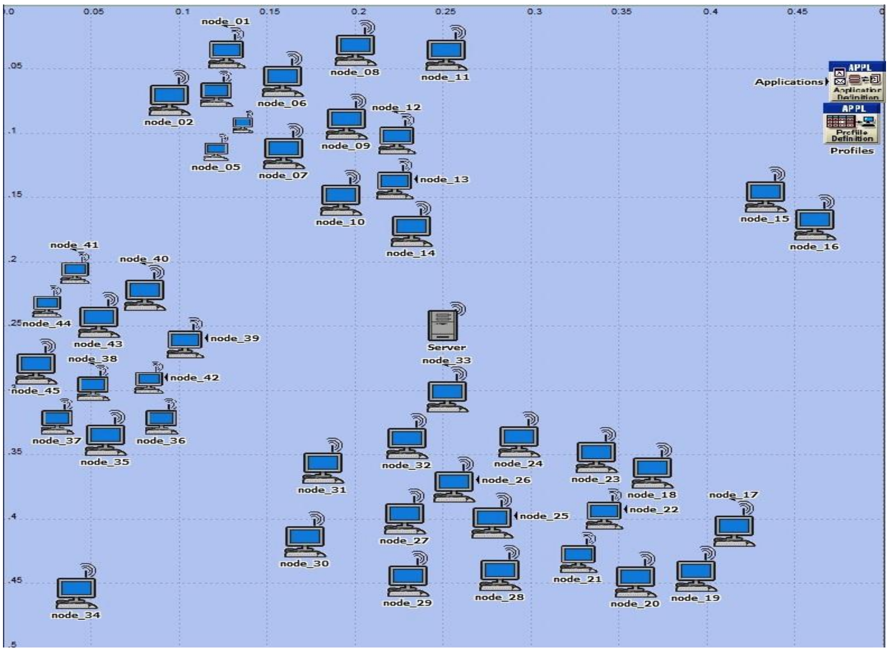
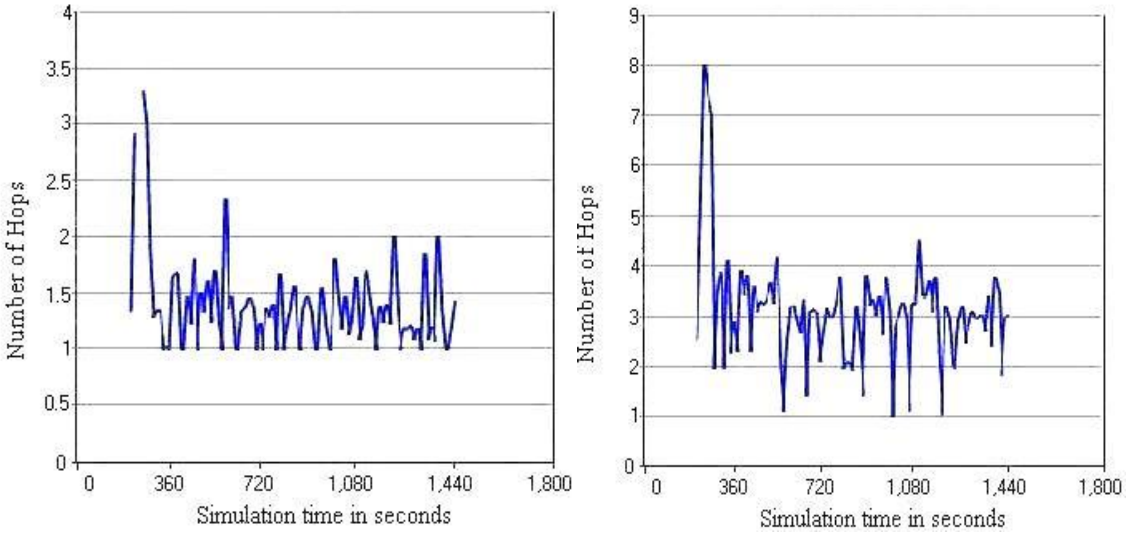


Figure 4.51: NAN with 49 nodes in a random structure

We built the network in such a way to be able to test how would respond some nodes which are from the rest "community". Moreover we placed two nodes in a distance from the Server and from the rest nodes greater than their range. The reason for doing this was that we wanted to check what their attitude is while they are not able to deliver their packets.

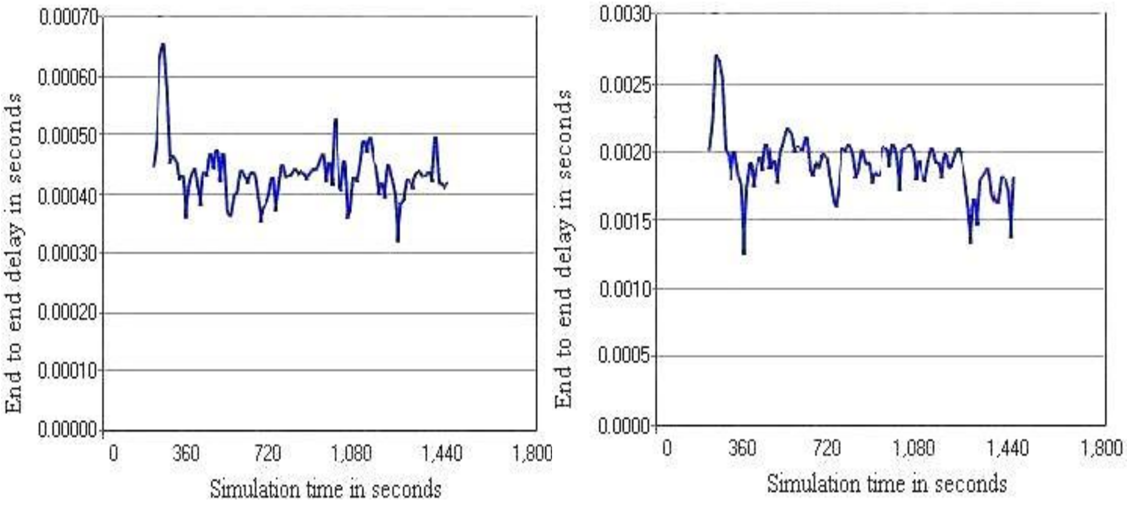
Initially, running the simulation setting as data rate 11Mbps, we see that the number of hops in average is very satisfying. Actually we see that this number does not overcome the value of three per route which is actually very efficient for that kind of networks. When the data rate of 11Mbps is implemented we can see that the number of hops increases and it has as a mean for almost the total simulation two to four hops.



(a) (b)

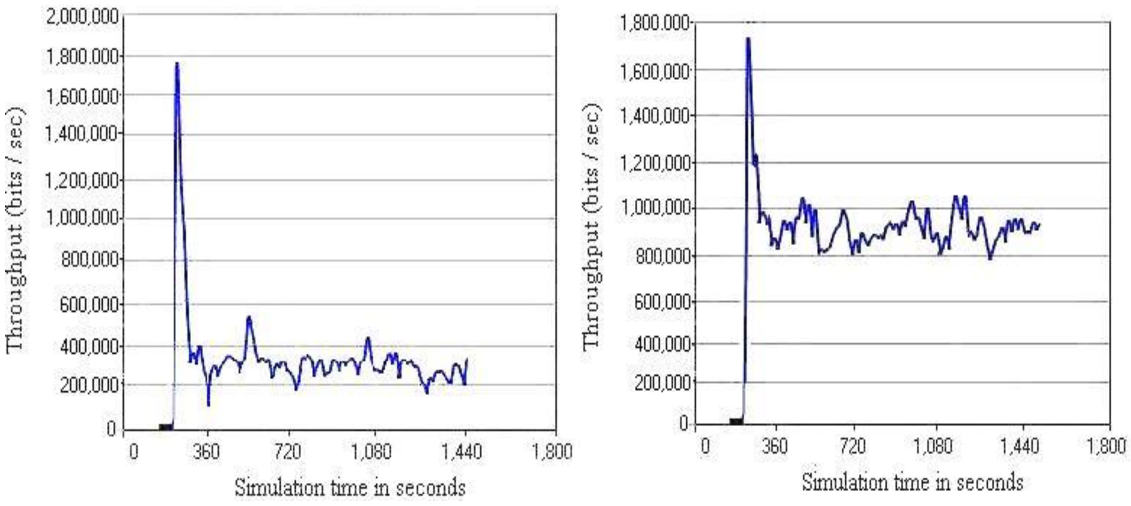
Figure 4.52: Number of Hops in a random topology for a) 1Mbps and b) 11Mbps

Of course we could not expect anything less than before regarding to the throughput and the end to end delay across the network. As it is shown and below the growth of the data rate creates more demands and that has as a result both throughput and end to end delay to get higher values.



(a) (b)

Figure 4.53: End to End Delay in a random topology for a) 1Mbps and b) 11Mbps



(a) (b)

Figure 4.54: Throughput in a random topology for a) 1Mbps and b) 11Mbps

The interesting topic in this network is, as we mentioned before, the way the remote nodes (node15, node 16) react to this situation. Figure 4.55 depicts their behavior during the simulation. They are trying many times to transmit their undelivered data. However since they cannot contact to any other node but for each other, they transmit their data between themselves without succeeding to reach further hops for their routes.

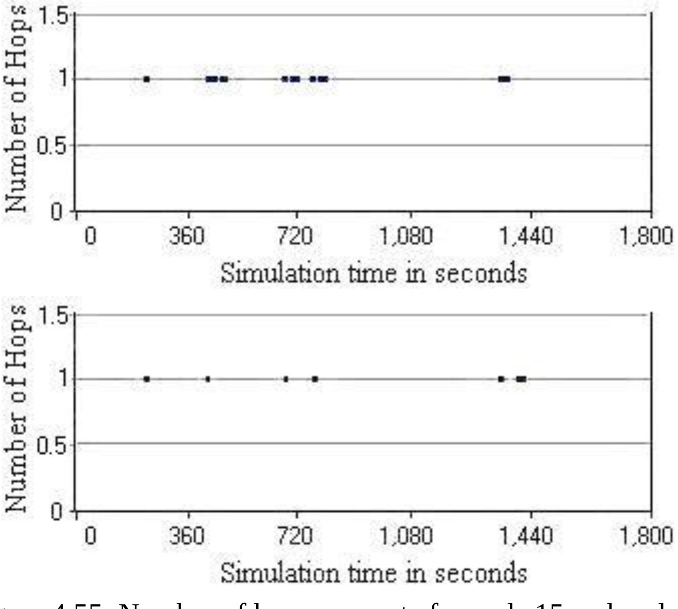
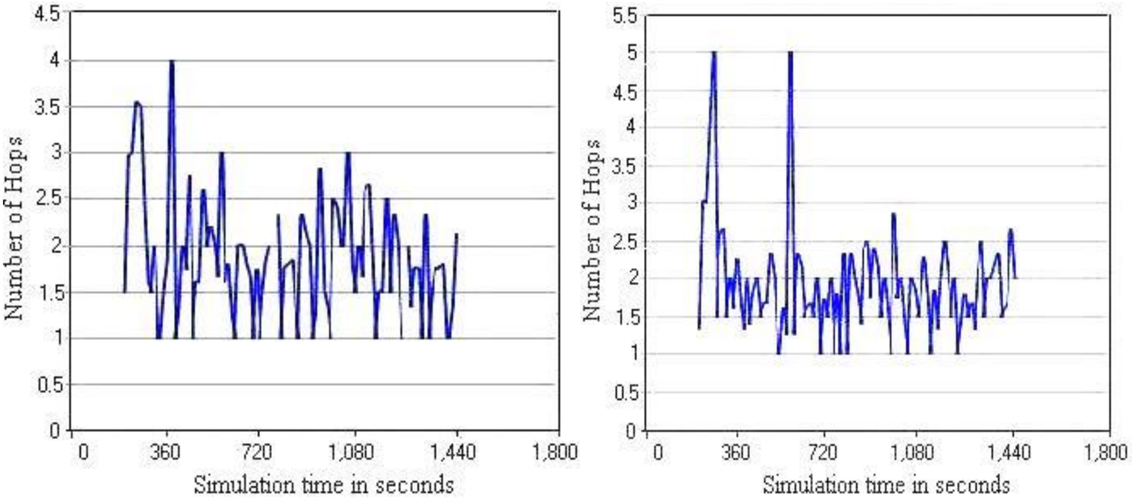


Figure 4.55: Number of hops per route for node 15 and node 16

Finally, we placed one further node in a remote location but its range includes other nodes of the network. That node needs obviously more hops per route than the average one for its data to be delivered successfully. What is more, it is affected by the increase of data rate too as we can see by the demands of its routes concerning the hops.



(a) (b)

Figure 4.56: Number of hops per route for node 34

4.2.3 Scenario 3

In this scenario we tested another routing protocol according to the parameters we investigate. First of all, our purpose was to find out which one would be more efficient for a random topology. Consequently, running a simulation for the same time we extract the following results.

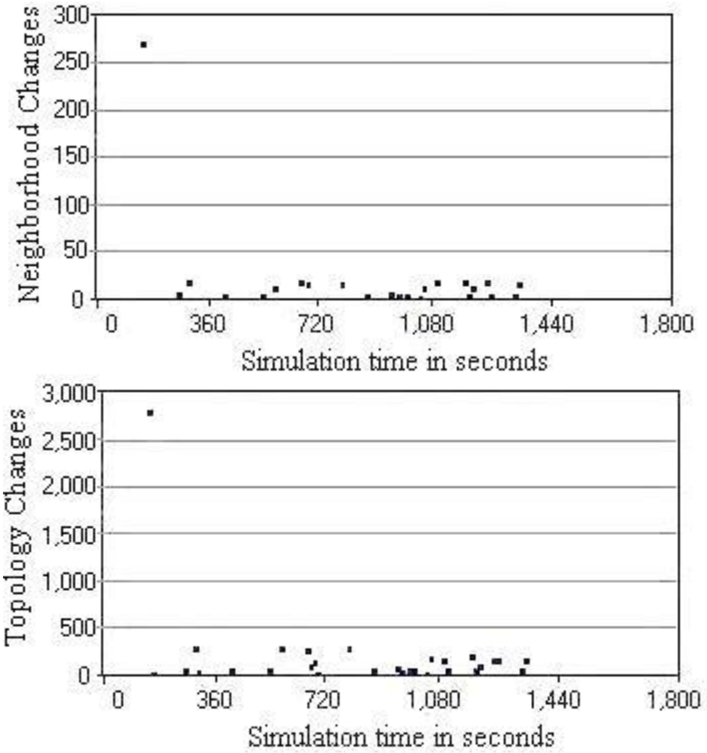


Figure 4.57: Neighborhood changes and topology changes

Above we can see that even in a fixed network there is a great variety and alteration on nodes' neighborhoods. About twenty to thirty such changes happen during the simulation which is a vast demand for the specific network. Moreover, these changes cause many more changes as far as the nodes' topology which changes up to 300 times in some moments of the simulation causing heavy throughput to the network.

Nevertheless, the data that traverse within the network do not have great delays. However for a long period of time to the end of the simulation we notice that there is a failure. There is no traffic generated at all, along the network which shows us that the specific protocol is not as efficient as the AODV.

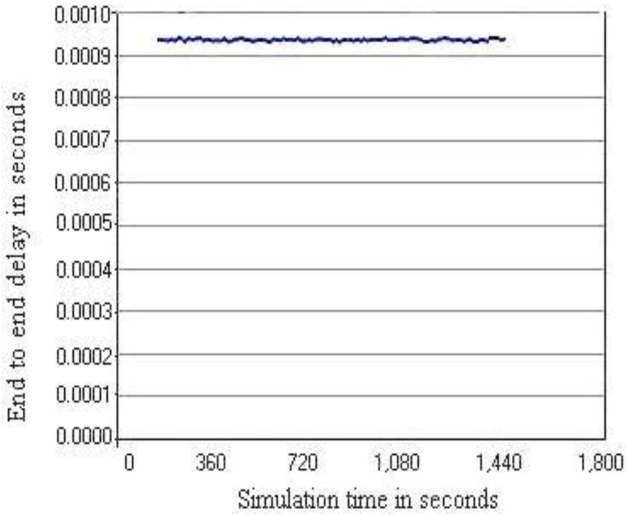


Figure 4.58: End to end delay

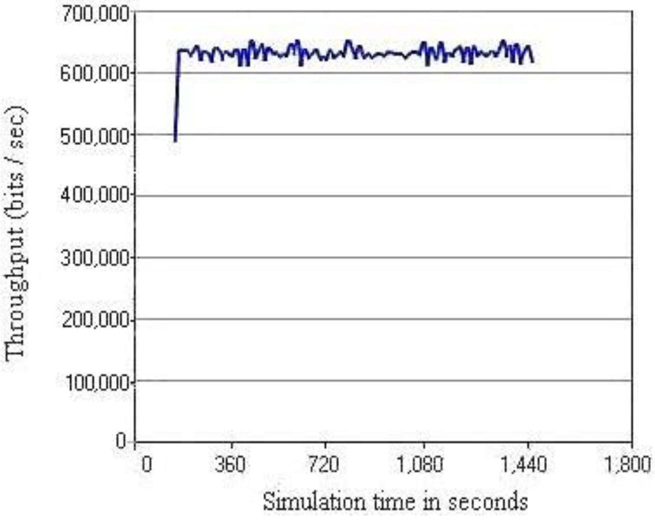


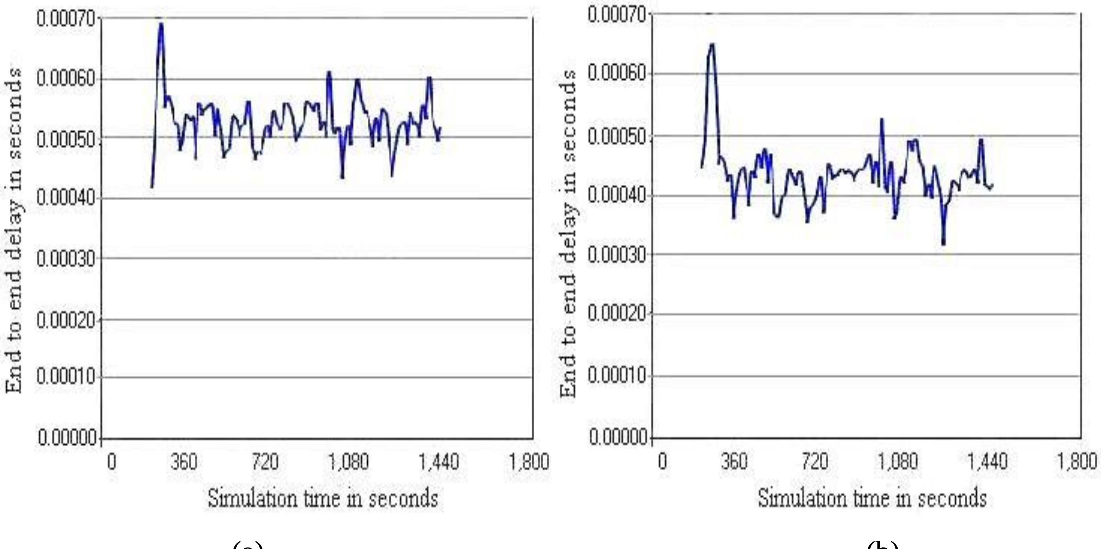
Figure 4.59: Throughput

4.2.4 Scenario 4

By this scenario we intended to investigate how a propagation model could affect a network. Obviously, all the available networks that we have built, they are not the most indicative for that purpose since there are not obstacles to study specific characteristics of the propagation models we set and their attitude. Nevertheless there are slight differences in our parameters however we cannot extract safe conclusions from these results.

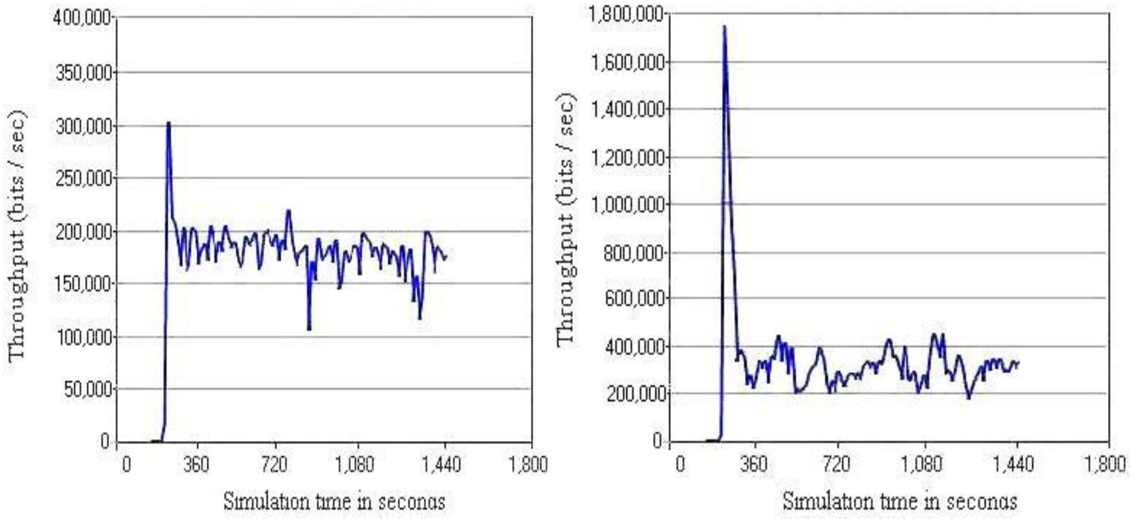
The propagation models that we implemented were Okumura Hata formula and Free Space Loss.

The network that these models were applied is the one with the random topology, which is depicted in Figure 4.51. Comparing our parameters there is a great difference only concerning the throughput. We notice that the mean throughput applying the FSL is two hundred thousand to four hundred thousand bits per second while the relative one applying the Okumura Hata formula is one hundred thousand to two hundred thousand bits per sec.



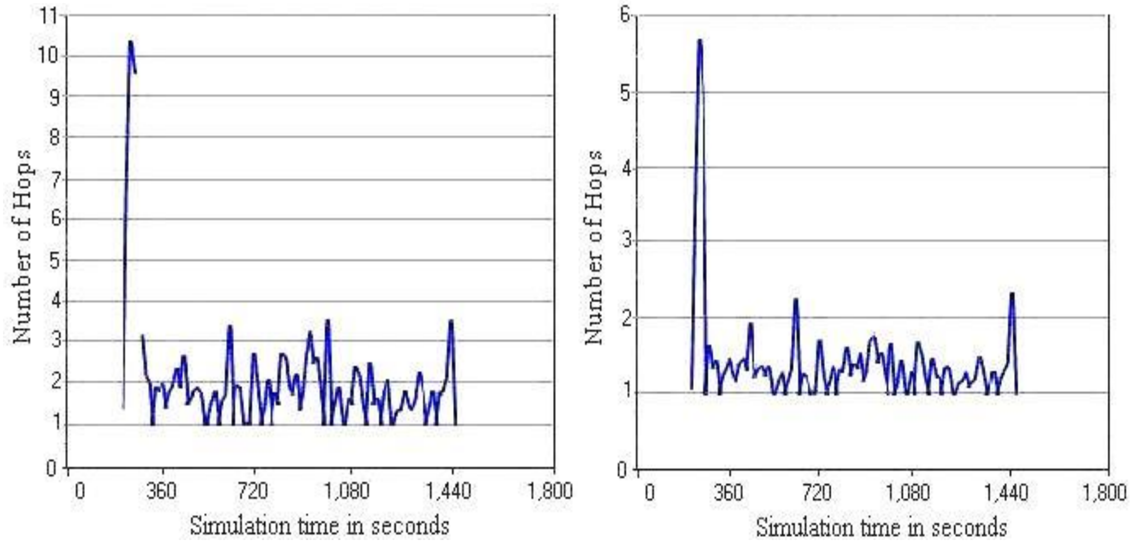
(a) (b)

Figure 4.60: End to end delay with a) HATA and b) FSL



(a) (b)

Figure 4.61: Throughput with a) HATA and b) FSL



(a) (b)

Figure 4.62: Number of Hops per route with a) HATA and b) FSL

5 Conclusions

The current dissertation is focused on providing a comprehensive investigation on the performance of Home Area and Neighborhood Area Networks operating in 868 and 800 MHz respectively using two different protocols 802.15.4 and 802.11. The project concentrates on calculating and predicting possible malfunctions and difficulties in such area networks. The simulations that have been run has the perspective to explore an optimal way of planning, building and operating an efficient network topology capable of dealing with the circumstances and requirements of every Area Network. It highlighted and proved “grey” areas of functionality that should be not implemented in such topologies. Moreover, it enhances the successful scenarios and their results.

This detailed performance was based on a detailed study of RF protocols and their operation. A detailed report of their characteristics and their requirements and of course a detailed analysis of their behavior in an Area Network is included, too. The main purpose was to identify if it is feasible to adjust all these with the appropriate smart meters in a topology so that Advanced Metering infrastructure to be feasible.

Undoubtedly, AMI has many benefits to provide with as far as the energy consumption is concerned. However there are some issues that should be taking under consideration. Initially, a manner should exist to combine two different protocols for NAN and HAN or finding a new one that could be applied efficiently enough in both of them. Moreover, it is necessary such an infrastructure to be able to predict how it will confront the continuous expansion of the initial topology so that it will be prepared to avoid the failure. Finally, it is absolutely necessary that infrastructure to have the flexibility to be configured according to the requirements it meets occasionally (density, decentralization of a coordinator, a different topology may serve better the network after some particular time, etc)

To conclude with, there are a lot of other issues that a further investigation should take place. The major concern is the security issues in exchanging data from network to network.

Bibliography

[1]M. Nabeel, J. Zage, S. Kerr, E. Bertino, N. Athula. Kulatunga, U. Sudheera Navaratne, M Duren, Cryptografic Key Management for Smart Power Grids, *Approaches and Issues*, 22/02/2012

[2]Price, *"Fundamentals of Wireless Networking"*, McGraw-Hill Irwin

[3]J. Moy, *"OSPF Version 2"*, IETF, RFC2328, April 1998

[4]J. Venieris, E. Nikolouzos, *"Network technologies"*, Tziolas.

[5] IEEE Standard for Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks Specific requirements- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), October 2003.

[6] Sinem Coleri Ergen. Zigbee/ IEEE 802.15.4 Summary. September 2004.

[7] Luis Carlos Aceves Gutiérrez,Og Jamir Ramos Juraidini,Carlos Alberto Garza Frias, *"Wireless control of Bluetooth "on/off" switches in a smart home using J2ME in Mobile Phones and PDAs"*.

[8] Matt Maupin, ZigBee: Wireless Control Made Simple.

[9] Patrick Kinney, *"ZigBee Technology: Wireless Control that Simply Works"*.

[10] Mikhail Galeev, *"Home networking with Zigbee*".

[11] Yu-Ping Tsou, Jun-Wei Hsieh, Cheng-Ting Lin, Chun-Yu Chen, *"Building a Remote Supervisory Control Network System for Smart Home Applications*", IEEE International Conference on Systems, Man and Cybernetics, Volume 3, Oct. 2006.

[12] Byoung-Kug Kim, Sung-Kwa Hong, Young-Sik Jeong, Doo-Seop Eom, *"The Study of Applying Sensor Networks to a Smart Home*", Fourth International Conference on Networked Computing and Advanced Information Management, Volume 1, Sept. 2008.

[13] A Zensys in constant development, Z-Wave Alliance Day Technical Seminar,

[14] Mikhail Galeev, *"Catching the Z-Wave"*.

[15] Z-Wave Overview presentation, 2008.

[16] ZENSYS Inc., *"Article: Z-Wave, The Wireless Control Language"*.

[17] Kazem Sohraby, Daniel Minoli, Taieb Znati, *"Wireless Sensor Networks, Technology, Protocols, and Applications"*, Wiley Interscience, 2007.

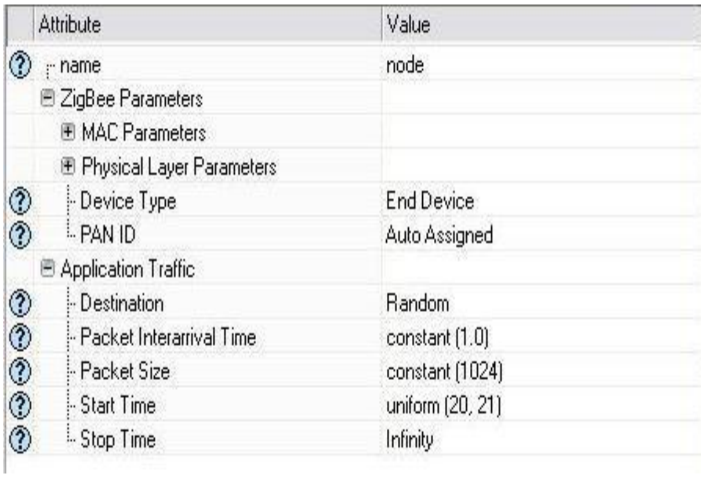
[18] Edgar H. Callaway, *"Wireless Sensor Networks: Architectures and Protocols"*, CRC Press 2004.

[19] Rajeev Shorey, A. Ananda, Mun Choon Chan, Wei Tsang Ooi, *"Mobile, Wireless, and Sensor Networks: Technology, Applications and Future Directions"*, IEEE Press, Wiley Interscience, 2006.

[20] Andrew S. Tanenbaum, *"Computer Networks, Fourth Edition"*, Pearson Education, 2003.

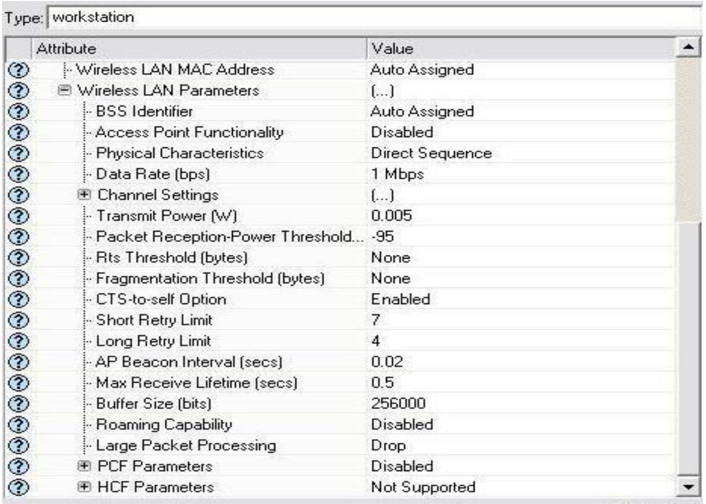
Appendix

There are available the attributes that are able to be configured for the nodes in the simulated networks. They are shown indicatively with their default values since they can be configured in which way we want to implement our network.



Attribute	Value
name	node
⊟ ZigBee Parameters	
⊞ MAC Parameters	
⊞ Physical Layer Parameters	
Device Type	End Device
PAN ID	Auto Assigned
⊟ Application Traffic	
Destination	Random
Packet Interarrival Time	constant (1.0)
Packet Size	constant (1024)
Start Time	uniform (20, 21)
Stop Time	Infinity

Picture 1: End device’s attributes ZigBee

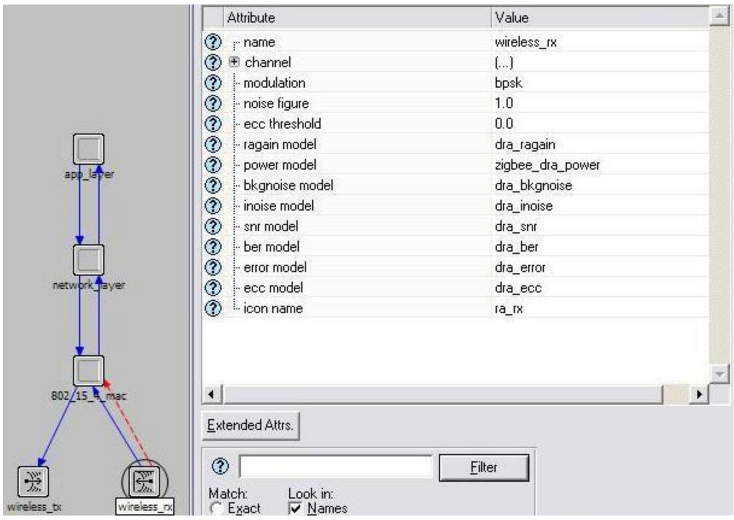


Type: workstation

Attribute	Value
Wireless LAN MAC Address	Auto Assigned
⊟ Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	1 Mbps
⊞ Channel Settings	(...)
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported

Picture 3: End device’s attributes 802.11

Except for the general attributes that we can configure, Opnet gives us the opportunity to change some settings in the layers (application, network, physical, etc). We are able to configure the default structure or even building a totally new one if we are not satisfied from the existing ones and the way they interact. Moreover, we can decide if the settings on the transmitter and the receiver side will agree with the general ones or will be different.



Attribute	Value
name	wireless_rx
channel	(...)
modulation	bpsk
noise figure	1.0
ecc threshold	0.0
ragain model	dra_ragain
power model	zigbee_dra_power
bkgnoise model	dra_bkgnoise
inoise model	dra_inoise
snr model	dra_snr
ber model	dra_ber
error model	dra_error
ecc model	dra_ecc
icon name	ra_rx

Picture 2: TCP/IP attributes