INTERNATIONAL
HELLENIC
UNIVERSITY

Practical aspects of a wireless mesh network

Konstantinos Tsekos

SID: 3301110012

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

OCTOBER 2012

THESSALONIKI – GREECE

Practical aspects of a wireless mesh network

Konstantinos Tsekos

SID: 3301110012

Supervisor:	Prof. Konstantinos Tzaras
Supervising Committee Members:	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 main subject of the dissertation is: “Practical aspects of a wireless mesh network”.

In this dissertation we study the topologies that exist in ad hoc mesh networks. For every network topology there is a description and an explanation of operational principles, the main characteristics and the routing protocols that are used and these are followed by a comparative analysis. Furthermore, there is a description of advanced metering infrastructure (AMI), smart metering and standards/guidelines that exist in this new scientific domain.

The last part of the dissertation covers the case of networking an area with RF Mesh and reflects to the practical analysis. In this section several nodes are connected using different topologies and with embedded programming we made experiments in order to investigate the performance of the network. In our experiment we measured packet delays and packet losses, the QoS, the interference between neighboring nodes and finally the coverage of the network.

Konstantinos Tsekos

Date

Monday 29/10/2012

Acknowledgments

This master thesis wouldn't have been possible without the support and the guidance of my Supervisor Dr. Konstantinos Tzaras and the Assistant Professor Dr. George Koutitas. Without their knowledge and their assistance the result of this master thesis wouldn't be successful.

I owe my deepest graduate to my parents for their financial support and encouragement during my studies for the MSc in ICT Systems of the International Hellenic University. Finally, I am obliged to many of my colleagues and friends who always been there and boosted me morally.

Contents

1 Introduction

Nowadays, ad hoc networks are the ultimate frontier in wireless communication technology. These networks allow nodes to communicate directly to each other using wireless transceivers without the existence of a fixed infrastructure. This feature distinguishes ad hoc networks from the majority of the traditional wireless networks, such as cellular networks and wireless LAN, in which nodes (i.e. cell phone users) communicate with each other through base stations.

Ad hoc networks belong in the wide category of the Distributed Transient Networks where the nodes are not centralized but they have the ability to join and to leave the network whenever or to whatever point of the network they want. In ad hoc networks the presence of a central access point is not obligatory because all nodes can discover the existence of other nodes which are close to them in order to expand the network. The connections of an ad hoc network are being created through multiple nodes which play an important role during the data routing. These nodes not only forward their data but also data from neighboring nodes which is very important in cases where the transmitter and the receiver have no direct connection. [1]

The following image illustrates a typical ad hoc network.

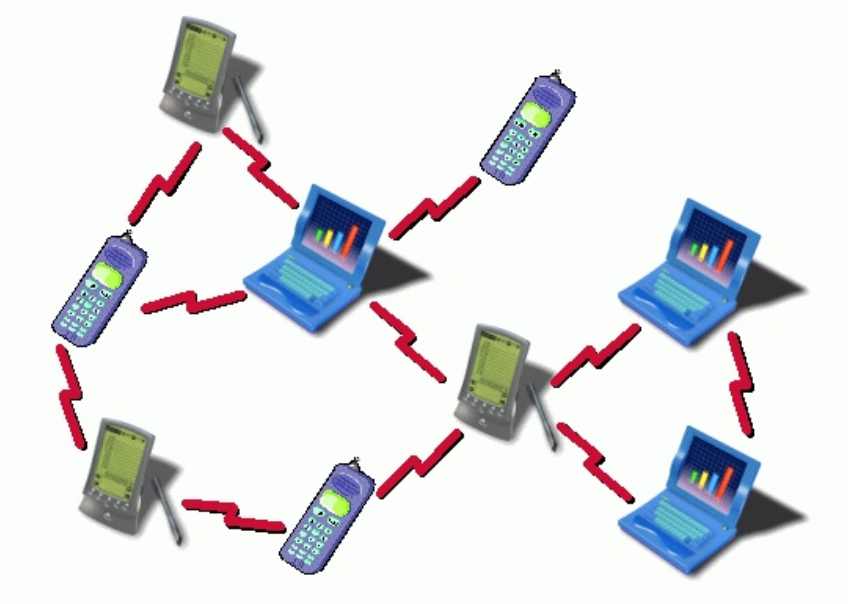

Figure 1.1 An example of an ad hoc network [2]

Furthermore, ad hoc networks can be divided into two categories:

- *Simple*. In this type of network, nodes use fixed transmission powers.
- *Power-controlled*. In contrast, nodes don't use a specific transmission power but they have the ability to change it. [3]

Power-controlled ad hoc networks are more popular because they have several advantages over the Simple ad hoc networks. The main advantage is that the energy consumption is significantly reduced because nodes can reduce the transmitted power when there is no need to transmit in high levels. Moreover, contention between the nodes can be reduced but also we can achieve an increase in the security of transmissions. When we detect high levels of interference we can reduce the transmitted power of some nodes in order to make more efficient our network.

Routing protocols play another important role in ad hoc networks. These protocols set the rules of how to establish a connection and how to forward the data even if some nodes are moving. The constant move of the nodes can create unpredictable scenarios in which routing protocols must correspond.

Ad hoc networks may be or may be not connected in the Internet and due to its mobility and also its unstructured nature it is easy to accommodate to new requirements. Furthermore, this type of network must have the ability to self-organize the addresses of the nodes and also to self-repair an unpredictable fault that may occur.

An ad hoc network is a network of computers which are distributed in the area and they communicate wirelessly through sensors. In the beginning ad hoc networks were used only for military purposes but later due to the rapidly development of the wireless communications, it was possible the construction of low cost and low power consumption wireless sensors. These sensors have the ability to identify the characteristics of the environment, to process the data and to communicate with other nodes in certain distances. For these reasons they are used in a variety of applications i.e. monitoring of the environment or home, medical applications, traffic control or home and industrial automation.

Furthermore, an ad hoc network is not only equipped with wireless sensors but also with a transponder, a microprocessor and usually a battery. The microprocessor is responsi-

ble to process and store the data that receives from the sensor. The transponder receives data from other nodes or the base station, and also transmits data to other nodes or the base station. The size of a node may differ from the size of a shoe box to the size of rice. Moreover, the cost of a sensor depends from thousands of euros to few cents. Due to the limitations of the cost and the size there are also limitations in the memory, energy consumption, range and processing power.

The main characteristic of an ad hoc network is the mobility. Nodes may move constantly and this is the reason why these networks were developed. The number of nodes is depending according to our needs and all nodes can connect and disconnect to the network randomly.

Moreover, another characteristic of ad hoc networks is the heterogeneity which means that there isn't only one type of device. It may include a group of mobile phones, PDA, laptops etc. which can communicate to each other. The distribution of the devices in the area depends on the network topology that will be chosen. For example, if the network extends to a large geographic area a multi-hop connection between the nodes is required.

In the next table the characteristics of an ad hoc network are presented.

Table 1: Characteristics of ad hoc networks.

HETEROGENEITY	**An ad hoc network in most cases is composed of heterogeneous devices.**
MOBILITY	**Almost all nodes in an ad hoc network have the ability to move.**
DISPERSED NETWORK	**Nodes can geographically be dispersed.**

Nowadays ad hoc networks are very popular due to the simplicity and the speed of the deployment of the network without requiring the existence of a fixed infrastructure. Another significant advantage is the dynamic nature of these networks which makes the process of adding or removing nodes very simple. Additionally, ad hoc networks are very secure and reliable due to the fact that all nodes are depending only on their neighbor nodes which makes difficult to an intruder to connect to the network. Heterogeneity

is very common in these networks because nodes may differ in processing power, range of transmission or battery life. Moreover, ad hoc networks may differ in a variety of features like if they can support multicast, broadcast or both, if they can connect and communicate with other networks, if they have static infrastructure and finally if they support the mobility of nodes and with what frequency.

In ad hoc networks the range of transmission of a node plays a very important role. If the range of the transmission is very big then the average number of data packet transmissions from a node to another node decreases. In contrast, a small range of transmission decreases the probability that a collision may occur and also the interference between neighbor nodes. This means that if we have a small range of transmission then we can have more transmissions simultaneously. Furthermore, the range of transmission plays a significant role in the battery consumption of every node which is a very important parameter in ad hoc networks. The range of transmission should be as small as possible in order to reduce the battery consumption but also we should not reduce it very much so that the network remains "connected". The most common choice is to choose a range of transmission every transmission to be "heard" by six nodes as we can see in figure 1.2.

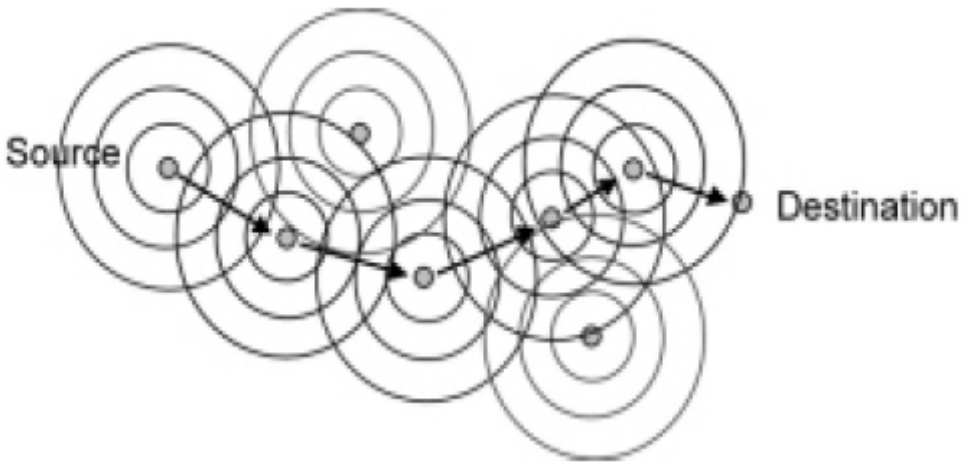

Figure 1.2 Range of transmission

In ad hoc network can be characterized by three levels. The first level is the Medium Access Control layer, which is responsible for the communication between the nodes in the physical medium. Route selection layer is the next level which is responsible for

finding the best route in order a packet to reach the destination. Finally, the last layer is the Scheduling layer which determines the sequence of data packet transmissions.

One of the most significant problems in ad hoc networks is routing. This is due to the fact that most of the routing algorithms were designed to operate in certain circumstances which are better than the reality that exist in ad hoc networks. The biggest problem that routing algorithms must face is the movement of the nodes which may be continuous. This feature can change the network topology and as a result routing algorithms must discover new data routes. Furthermore, due to the limited range of transmission, the number of transmissions of messages that are relevant to routing decisions must be very small. In ad hoc networks, the percentage of packet losses is very high due to the high probability of transmission errors, and the fail of a data path. As a result we should choose a routing protocol which is distributed, and every node is intelligent enough in order to take routing decisions. A centralized routing protocol is not reliable and efficient enough when the nodes are moving constantly. Moreover, the routing protocol should take under consideration the energy level of every node before taking a routing decision.

There are many challenges to be solved in order to exploit all the features and the advantages of ad hoc networks. We can list these challenges as follow [4]:

- *Energy consumption.* In most cases, ad hoc networks are equipped with batteries which results to try to achieve to use this limited energy as efficient as possible.
- *Time varying network topology*. Since all nodes in an ad hoc network can move and change place it is difficult to have a structured network topology. As a result, in these conditions the optimization of performance is complicated.
- *Low quality communication.* It is widely known that wireless communication lacks in quality from wired communication. Moreover, ad hoc networks are affected from environmental factors i.e. obstacles, weather conditions, interference, etc. which have a big impact in the QoS.
- *Scalability.* Most of the routing protocols, that were design for ad hoc networks, operate efficiently in ideal conditions and with a specific number of nodes. That doesn't mean that these protocols will still be efficient in all conditions and in the presence of a large number of nodes.

- *Resource constrained*. Scarce resource availability is something that happens very often in ad hoc networks. Energy and bandwidth are limited in these networks so protocols should try to find ways to provide the desired performance with the available resources.

These challenges will be explored via the experiments that will take place in indoor and outdoor environments. Figure 1.3 shows the wireless sensors that were deployed in a home area network (HAN) and more specifically in International Hellenic University (IHU).

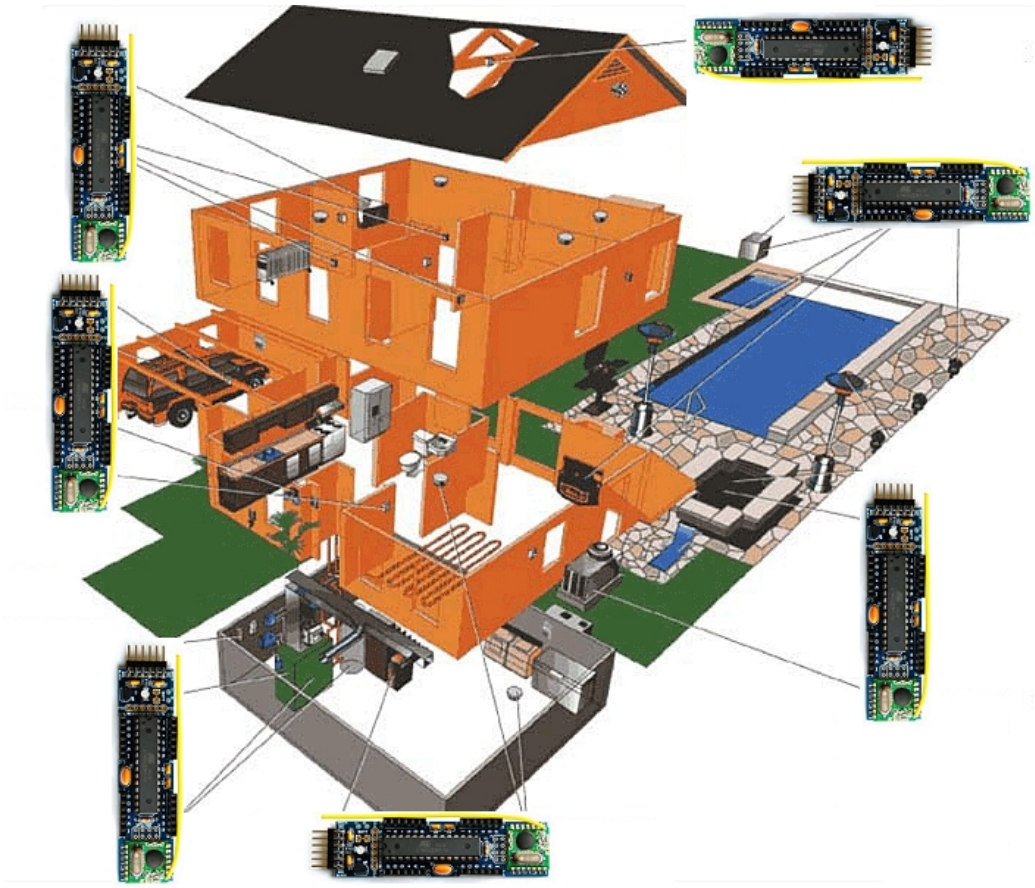

Figure 1.3 Wireless Sensors in a HAN

These sensors were deployed using different network topologies or environmental conditions and with embedded programming every node was able to send and receive data from neighboring nodes. Furthermore, several experiments were performed in order to measure specific characteristics of the network such as the packet delays and packet

losses, the QoS, the interference between neighboring nodes and finally the coverage of the network.

The results of all these experiments were taken under consideration in the implementation of a mesh protocol that it can connect the sensors using the channel and the RAM of every sensor as less as possible.

The second chapter describes existing network topologies for ad hoc mesh networks and also presents the characteristics of each topology. Chapter three describes the Standards in Advanced Metering Infrastructure which provides the framework in order to achieve smart grid interoperability. In chapter four there is a description of how to connect multiple nodes with RF Mesh protocols. Furthermore, a series of experiments will be presented in order to investigate the performance of the network and problems that usually occurs. Finally, in chapter five there is a demonstration of the RF mesh protocol that was implemented.

2 Network Topologies for Ad Hoc mesh networks

Network topology refers to the shape of the network or the network's layout. A network topology explains to us how different nodes (computers, hubs, routers etc.) connect to each other and how they communicate to each other in order to create a network. Network topologies are divided into two categories, physical or logical.

Physical topology is the way that different nodes are connected through the physical medium which is the actual cables. In contrast, the logical topology is the way that the data passes through the physical medium from one node to another node without taking under consideration the physical interconnection of the nodes. It is not necessary that the logical topology should be the same with the physical topology in a network.

Topologies play an important role in network design theory. In order to build a computer network in a home or in a business area we must take under consideration the characteristics that our network should have, what tasks should perform and how we can achieve them via different network topologies. As we can imagine every network topology has different characteristics and different advantages and disadvantages. So, we must first fully understand what tasks our network should perform and what characteristics should have and then we should try to investigate which network topology corresponds to them. In order to do this we must first know in depth every aspect of every network topology. [5]

The network administrator should weigh the pros and cons of different topologies and to choose the one that is more efficient to his needs. In order to take this decision network administrator should think between these aspects:

- planned applications and data rates
- required response times
- type and number of equipment being used
- cost

Two networks may have the same topology if the connection that is configured is the same although the distance between the nodes or the transmission rate may differ. In the following paragraphs every topology will be presented in detail.

The simplest wireless network topology that exists is the line topology. In this topology two or more nodes are connected directly to each other (Peer to Peer) using the same channel (Figure 2.1). There aren't any alternative data paths and when a direct data path doesn't exist then the node must send its data to its neighbor node and then this node will forward to its neighbor or to the destination. Furthermore, in this topology there isn't any access point which can control and manage the entire network. Line topology is not scalable and this is the main reason why is not very popular in ad hoc mesh networks.

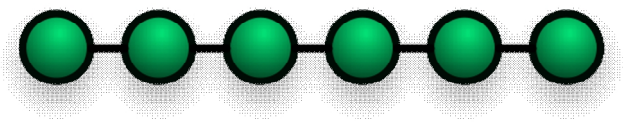

Figure 2.1 Peer to Peer connection

The most popular topologies in ad hoc mesh networks which will be presented in the following paragraphs are:

- Star topology
- Tree topology
- Mesh topology
- Combined – Hybrid topology

2.1 Star Topology

2.1.1 General Description

Star topology nowadays is the most common network topology in businesses but also in home networks. In star topology nodes are divided into two categories and they can be a

peripheral node or a central node. In this topology every node will connect to a central node which can be a hub or a switch. Star topology is very easy to manage and this is the reason why is so popular. Figure 2.2 is a typical example of the star topology.

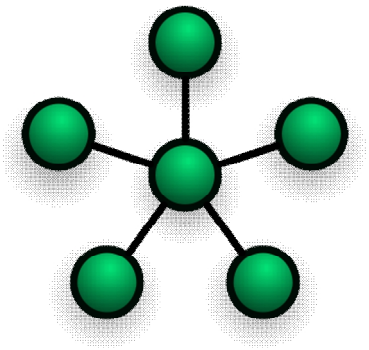

Figure 2.2 Star Topology

When a peripheral node wants to communicate with another peripheral node, then the data that he wants to send should be sent first to the central node and then the central node broadcasts the data to all peripheral nodes. In some cases the central node broadcasts the data to all peripheral nodes including the node that transmitted this data. In this example we call the central node passive and the peripheral node should be able to tolerate any echo that it has received from its own transmission. If we want to prevent echo-related problems then we use an active central node which can decide to whom he will send the data.

In star topology every peripheral node can communicate with another peripheral node through the central node. As a result if a transmission line of a peripheral node fails then this node is isolated from the network but the rest network can still operate. This node hasn't the ability to communicate and also the rest network can't reach this node. In the worst scenario that a central node fails then the entire network fails and all nodes are unreachable.

Star topology can be divided into two categories. The first category is the extended star topology. In this case there aren't only the central node and the peripheral nodes but also there are transmitters in order to extend the maximum transmission rate between the central node and a peripheral node. The extended star topology is used in order to break the limits of the distance between the nodes. In the distributed star topology there are

the central node and the peripheral nodes but the main difference is that a peripheral node may be connected to other nodes. As a result if these nodes want to communicate with another peripheral node of the network then they transmit their data to the peripheral node that there are connected and then this peripheral node will transmit the data to the central node which is responsible for the broadcast of the data. [5]

2.1.2 Characteristics of Star Topology

As it was said before, star topology is very popular and the reason why is the advantages of this topology compared to the others. When a node wants to communicate with another node then at most three nodes and two links are involved in this communication. As a result there is no participation of a large number of nodes but only the participation of the central node and the two peripheral nodes. Although a node can monopolize the central node, there are techniques that can prevent this case. Another advantage of star topology is that every peripheral node is isolated by the link that connects it to the central node. If that links fails that doesn't mean that the entire network will fail which happens in other network topologies. Star topology is very centralized and when the capacity of the central node is increased or more nodes are connected the size of the network increases. Moreover, the addition or the remove of nodes isn't sure that it can cause a disruption of the operation of the network. The entire network can still operate without any problem. Finally it is very easy to detect any faults that appear to the network and to solve it.

On the other hand, star topology is depending on the functionality of the central node and as a result any fault that may appear to this node has huge consequences to the entire network. This is the worst case scenario but every network administrator should take it under consideration.

In the following table we can see a summary of the advantages and disadvantages that the star topology has.

Table 2: Characteristics of Star Topology.

Advantages	**Disadvantages**
Easy to add new workstations	Hub failure cripples all workstations connected to that hub

Centralized control	Cost of central nodes
Centralized network monitoring	

The star topology can be found in Hotspots, Telecenters, Offices and WISP's (Figure 2.3).

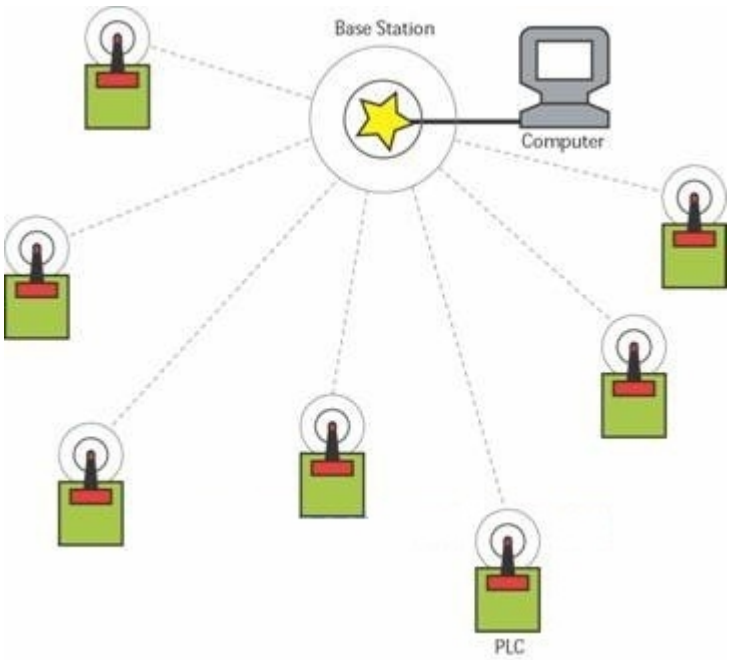

Figure 2.3 Example of Star Topology

As the image above shows, there are seven wireless workstations, one base station and one computer which is connected to the base station. Every workstation is connected wirelessly with the base station in order to get access to the Internet. Through the computer the settings of the network can be changed i.e. change in the protocol that is used or delete of a workstation. [5]

2.1.3 Routing Protocols

The most common routing protocols which are used in a star network are:

- **SimpliciTI** which is suitable for a network which contains two to thirty nodes. Only endpoints can sleep and the data rate is approximately 100 kb/s. [6]

- **TI-MAC** is suitable for larger networks which can contain two to one hundred nodes. This protocol can support both beaconed and non-beaconed modes. In beaconed mode only endpoints can sleep, in contrast in beaconed mode all nodes can sleep. With this protocol data rates of more than 100 kb/s can be achieved. [7]
- **RemoTI** is not very popular and it is suitable for only small networks with two to ten nodes. It is used most in the audiovisual market and in order to accommodate RF remote controls to consumer electronics devices. [8]

2.2 Tree Topology

2.2.1 General Description

Tree topology is a combination of the star topology and bus topology. This type of network topology consists of a central node which is connected to one or more leaf nodes, which are one level lower in the hierarchy of the network with only one point to point link between the central node and each one of the second level node. The nodes in the second level may also be connected to nodes in a lower level of hierarchy (third level) with a point to point link and this means that only the central node isn't connected with any node above it in the hierarchy. As a result when a node wants to communicate with another node that hasn't the same parent, then it has to communicate with nodes which are above it in the hierarchy and especially with the central node. The structure of this network is like a tree, in which when a leaf from a branch wants to communicate with a leaf to another branch then it should send its message to the above branches then to the tree trunk and finally to the branches that the receiving leaf belongs (Figure 2.4).

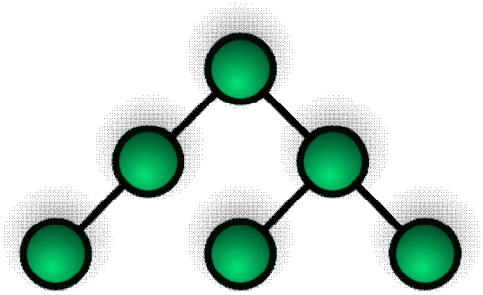

Figure 2.4 Tree Topology

Moreover, in tree topology there are some communication rules that are followed from every node. Every child node can communicate only with its parent node and with no one else. When it wants to communicate with another node (not his parent) then it should forward its message to its parent and the parent node decides to whom it will forward. A parent node can only communicate with its children and its parent node.

In tree network topology at least three levels of hierarchy must exist and all nodes in every level operate according to the root node. Furthermore, in tree topology there are two ways of connecting the nodes, the linear and the star. The network functions by taking into account the total number o nodes that exist and it doesn't matter how many nodes are in every level. In most cases nodes that are in higher level of hierarchy are more intelligent and perform more functions. [5]

2.2.2 Characteristics of Tree Topology

Like every network topology, tree topology has advantages and disadvantages and it is used in cases when the benefits from the features that it has are important. Tree topology is more suitable in large networks where star and ring topologies are not efficient. In this scenario where the network is large enough with star or ring topology there is high probability of large delays and moreover a node can monopolize the entire network which can be avoided with tree topology. Another feature of this topology is that the network can be divided in parts and as a result it becomes more efficient and more manageable. Moreover, there is no limitation in adding or removing a child node and also it can be done without interrupting the operation of the network.

On the other hand, the addition of more nodes to the network makes it more complicated and it is difficult to manage it. So, it should always take under consideration the complexity of the network when there is a need for a new addition. If a data-link or a node fails and an alternative route doesn't exist, a big part of the network may become isolated. Furthermore, the network is wholly dependent on the root node and this means that a failure in this node will collapse the entire network.

It is very important to mention that the tree structure suits best when the network is widely spread and divided to many branches. This allows the existence of many servers something that is very useful for universities, schools and colleges so that each branch can identify the specific system of the network. Figure 2.5 shows a tree network in a

home area where every room is a leaf or a branch. The roof is the central node of the network.

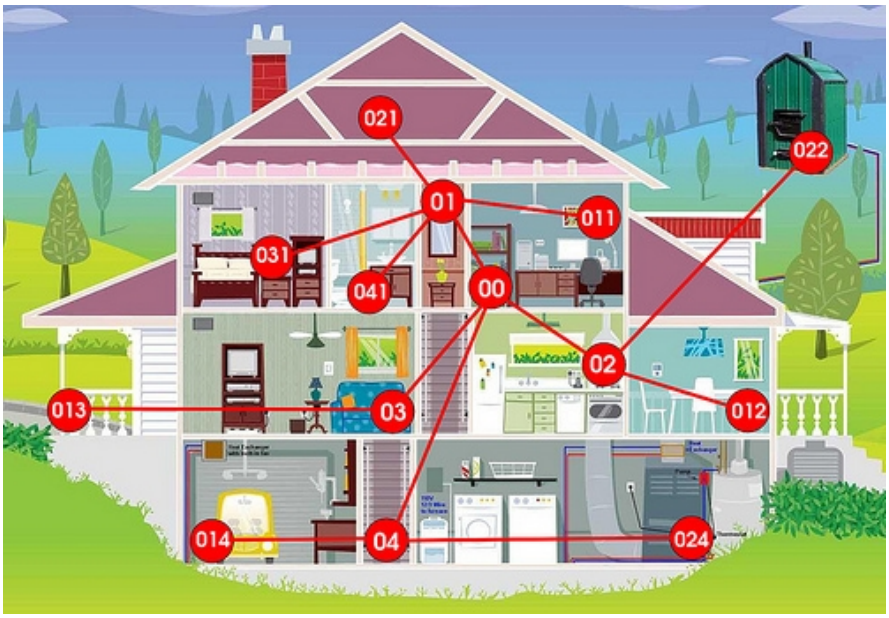

Figure 2.5 Example of Tree Topology

2.2.3 Routing Protocols

The most common routing protocol that is used in tree network is the spanning tree protocol (STP). STP can guarantee path redundancy but also it can prevent loops which may exist due to multiple paths between the nodes. When two nodes wants to communicate, STP according to the cost of every path between these two nodes, chooses the path with the lowest cost and put the others in a standby or blocked state. In this case only one path is active at a certain time between two nodes, but all the other paths are kept as a backup if the active path collapses or the cost increases. If the active path fails or the cost increases then one of the backup paths will be chosen to connect the nodes.

There is a problem that STP didn't solve and this is the "data loop". A data loop exists when two or more nodes on a network can transmit data to each other over more than one data path. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, which needlessly consume network bandwidth and can significantly impact the performance of the network.

Rapid Spanning Tree Protocol (RSTP) can prevent data loops from forming which ensures that only one data path exists between the end nodes in the network. Where multiple data paths exist, this protocol places the extra paths in a standby or blocking mode, leaving only one main active path.

Furthermore, RSTP can also activate a redundant path if the main data path goes down. So not only RSTP protects the network from broadcast storms, but it can also maintain network connectivity by activating a backup redundant path in case a main link fails.

When a change is made to the network topology, such as the addition of a new node, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

RSTP can complete a convergence in seconds, and so greatly diminishes the possible impact the process can have on the network.

2.3 Mesh Topology

2.3.1 General Description

In mesh topology all nodes are interconnected to each other. There is no specific way about how to connect nodes or which node to connect with another node, like the topologies that were described before, but the connection of the nodes is depending on the needs of the network. Moreover, in a network which uses mesh topology every node is connected through hops, some may be connected through a single hop and others may be connected through more than one hop as it can be seen in Figure 2.6.

Mesh topology is a special type of network topology where the nodes not only receive and transmit their data, but also receive and retransmit data which have as a destination other nodes. That means that nodes in this topology work as a relay for other nodes. Furthermore, in order to have the propagation of data across the network all nodes must collaborate.

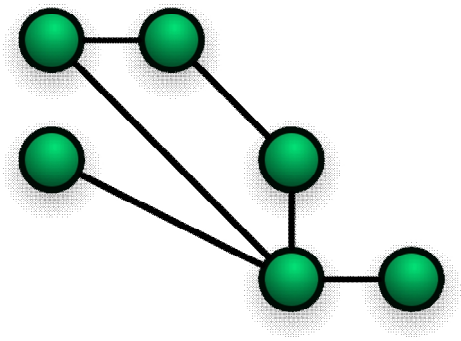

Figure 2.6 Mesh Topology

A network where all nodes are connected to each other is called “a fully connected network”. This is a rare example of a mesh network. In most cases a partial mesh topology is used which is more practical. In partial mesh topology some nodes are “indirectly” connected to other nodes.

Figure 2.7 is an example of a fully connected mesh network.

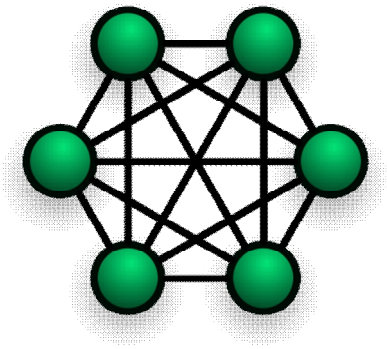

Figure 2.7 Fully connected mesh topology

Even if a node collapses that doesn’t mean that the entire network can’t operate. In mesh topology there is the “self-healing algorithm” that helps nodes in a mesh network to find alternative routes to transmit data in order to reach the destination. There are many routes that data can follow in a mesh network that it is very rare a failure in a node to cause the failure of the network. The case where all nodes of the network fail in a certain point of time is very unlikely. [5]

2.3.2 Characteristics of Mesh Topology

Mesh topology has a big benefit which is the redundancy. This means that even if a small number of nodes collapse this doesn't mean that the network can't operate. Another advantage is that multiple nodes can transmit and receive data simultaneously which can withstand high traffic. Moreover, when there is a need of adding or removing a node that doesn't mean that other nodes must be disrupted, but these nodes can still operate.

On the other hand, a big disadvantage of mesh topology is the high cost and this is the reason why mesh networks are deployed in areas that are unreachable and difficult to have a fixed network. Furthermore, the administration of a mesh network is very difficult and it gets more difficult when the network grows.

Mesh networks are very popular nowadays and are used in municipal networks (Figure 2.9), campus networks and neighborhood communities.

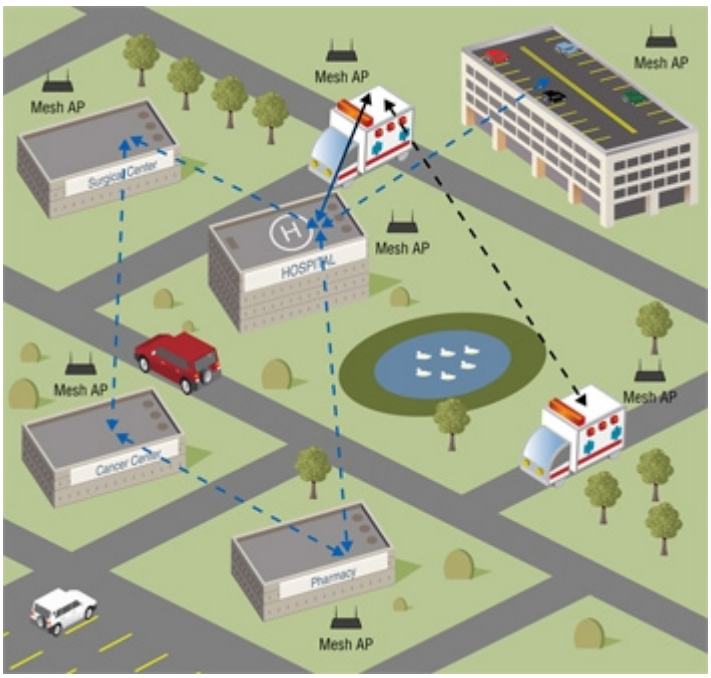

Figure 2.9 Example of a municipal mesh network

In this example there is a hospital with various departments which are connected to the central department or to the ambulances. In this way every department can be informed in real-time where an ambulance must go or to locate where a specific ambulance is.

Moreover, critical time is saved when a department wants to communicate with another or to the central department. [9]

2.3.3 Routing Techniques and Protocols

In order to reach the destination data travels through a number of hops which may be different even if the transmitter and the receiver are same. In mesh topology we can use two techniques in order to propagate the data and that techniques are:

- Flooding technique
- Routing technique

Flooding technique is the case that when a node wants to transmit data to another node then it sends the data to all of its neighbors and then these nodes retransmit the data to their neighbors until the data reach the destination. As a result the entire network is flooding with the data of the transmitter. This technique has many disadvantages but is very simple to implement. The biggest disadvantage is that a node can monopolize the network which can cause delays in the transmissions of other nodes, and in the worst case scenario some nodes will never transmit their data. This is known as "starvation problem".

Furthermore, in most cases data travels in the opposite way from where the destination is which should be avoided. In contrast, in routing technique the network is configured in such a way that data travels through the shortest path. This means that every node knows the topology of the network and it can decide to whom to forward the data. This technique is not simple to be implemented, especially when the network grows it gets more difficult, but with this technique the problems that flooding technique has can be avoided.

An example of a routing technique is the Ad hoc On Demand Distance Vector (AODV) routing algorithm which is capable of multicast and unicast. This protocol creates and maintains the data paths only when the nodes that want to communicate have data to send. In order to create a data path, AODV uses a route request and a route reply query circle. When a node wants to communicate with another node for which the route doesn't exist then it broadcasts a route request (RREQ). Every node that receives this RREQ may send a route reply (RREP) if this node is the destination or has a route to the

destination. If this is not the case, it will rebroadcast the RREQ. Furthermore, if a node receives again the same RREQ it can identify it from the source IP address and the ID of the RREQ and in this case the node will discard it and not broadcast it. [10]

Another example is the Topology Broadcast based on Reverse-Path Forwarding protocol (TBRPF) which can minimize the amount of update and control traffic required to maintain shortest (or nearly shortest) paths to all destinations. This is very important if the network changes frequent the topology or the link-cost, or if the nodes must use links of limited bandwidth, or if the network is very large. These problems are very common in wireless ad hoc networks.

TBRPF is a full-topology link-state protocol: each node is provided with the state of each link in the network (or within a cluster if hierarchical routing is used).

TBRPF uses the concept of reverse-path forwarding to broadcast each link-state update in the reverse direction along the spanning tree formed by the minimum-hop paths from all nodes to the source of the update. Moreover, each link-state update is broadcast along the minimum-hop-path tree rooted at the source of the update. The broadcast trees (one tree per source) are updated dynamically using the topology information that is received along the trees themselves, thus requiring very little additional overhead for maintaining the trees. TBRPF achieves reliability despite topology changes, using sequence numbers. [11]

Figure 2.8 shows how TBRPF protocol operates.

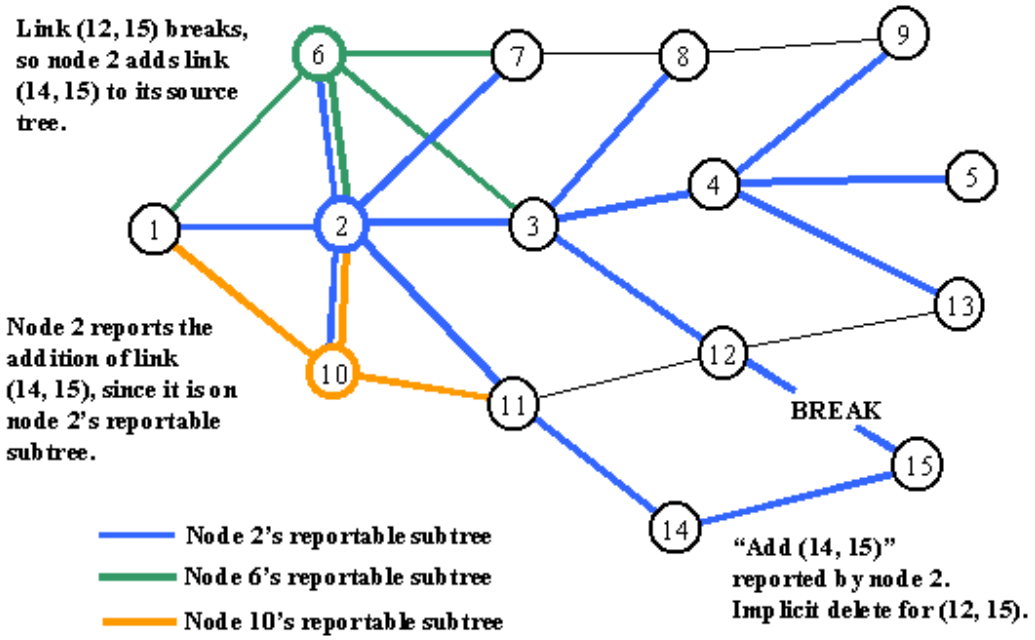

Figure 2.8 Operation of TBRPF protocol [12]

2.4 Combined Topologies

In previous chapters structured network topologies were presented and their characteristics were analyzed in detail. This chapter describes the combination of different structured network topologies in order to create a hybrid network which corresponds better to the needs of the network. Hybrid, as the name suggests, is a combination of different features, which as a result has the characteristics that can help to meet the needs that were specified while one network topology can't achieve this goal.

A hybrid network combines the best features of two or more structured network topologies which gives to the users a large number of routes that data can follow in order to reach the destination. The resulting hybrid network must not have the characteristics and the features of a standard network topology. For example, the combination of a tree network with another tree network isn't hybrid, but it remains a tree network because it still meets one of the standard network topology definitions.

The two most popular hybrid network topologies which will be presented in the following paragraphs are:

- Star-bus network topology (Figure 2.10)

- Star-of-stars or Hierarchical star network topology
- Star-mesh network topology (Figure 2.11)

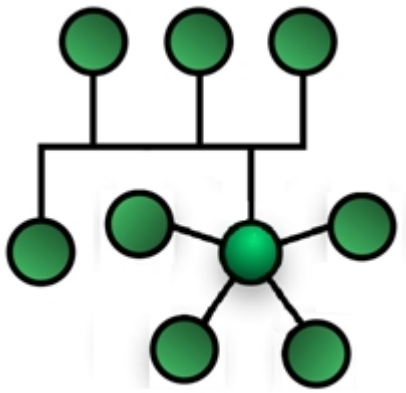

Figure 2.10 Star-bus Topology

In star bus topology the central nodes are connected through a bus topology and one or more of these central nodes are connected with peripheral nodes, which belong in a lower level, through the star topology. When one peripheral node wants to communicate with one of the central nodes then it must forward the data to its central node. The central node is the one who has a direct communication, as the previous image shows, with the other central nodes. That means it is central node's responsibility to forward the data to the destination.

The hierarchical star topology is a hybrid topology where there is an interconnection of individual networks which use the star network topology. In this case there is a central node which belongs in the top level and it is the administrator of the entire network. Furthermore, in this central node are attached second level central nodes, which may also be central nodes of third level star networks.

Star mesh topology has dual functionality which combines the speed of the star topology and the self-repairing capability of the mesh topology. In a star mesh network all nodes are connected to the central node and moreover there are direct connections between them. When two endpoints request a direct communication then the central node allocates to them the appropriate bandwidth which in this case endpoints don't waste the critical bandwidth of the central node. Figure 2.11 illustrates a star mesh network. The

purple nodes are the endpoints, the red are the routers and the green node is the central node. [5]

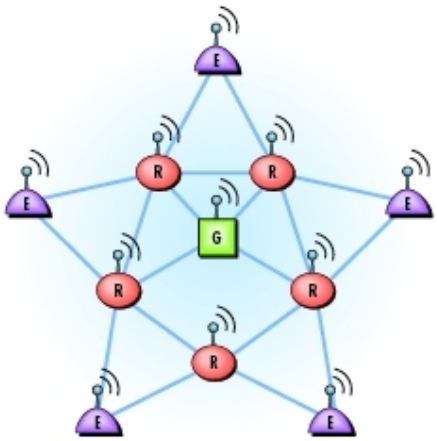

Figure 2.11 Star-mesh Topology

2.4.1 Characteristics of combined topologies

The biggest advantage of a hybrid network is the combination of the best features of two or more network topologies. A hybrid network can be designed in such a way that it corresponds better to the needs or the limitations that exist, which is very difficult to be done with one of the standard network topologies. Moreover, a hybrid network provides a large number of routes that data can follow which gives a benefit if high traffic must be accommodated. The failure of one or more nodes doesn't mean that the entire network can't operate because there are many data paths.

On the other hand, the cost of a hybrid network is very high because there is a need of intelligent nodes which can provide automatic fault-isolation and processing. These intelligent nodes are very expensive. Furthermore, a hybrid network is very difficult to be managed and it gets more difficult when the network grows. It is very complicated to extend a hybrid network, because there is a case that the addition of more nodes can totally change the features of the network which can make the network non-operational. As a conclusion, is not easy to design a hybrid network even for experienced network designers.

2.5 Comparative analysis of network topologies

As it was described in the previous paragraphs, every network topology has different features and as a result different advantages and disadvantages. None of these topologies is better from another in all cases but according to the needs the appropriate topology can be chosen.

Star topology is more centralized which makes it appropriate for a network which it is important to manage and to monitor it from a central node. On the other hand, tree topology is used in networks which are widely spread. In tree topology there is a classification and assignment of different privileges in every branch. This is the reason why it is adopted from most Universities, schools etc. The main characteristic of mesh topology is redundancy. A mesh network can still operate even if some nodes fail, but on the other hand the cost is a dissuasive factor. Mesh topology is used in cases where it is important to alleviate the high traffic or the nodes are constantly moving. Finally, a combined network topology includes the characteristics of different network topologies. As a result, this topology is not static but it can be changed according to the needs that were specified.

The following table is a comparative analysis of all network topologies that have been described in the previous paragraphs.

Table 3: Comparative Analysis.

Network Topologies	Advantages	Disadvantages
Star	• There is no disruption when we add or remove nodes. • It's simple to detect and to repair faults. • Centralized network topology.	• Cost of central nodes. • If the central node fails the entire network collapses.

Tree	• It is very efficient even for large networks. • It is more manageable. • We can add or remove child nodes without disrupting the operation of the network.	• The network is depending on the root node. • If a data path fails a big part of the network may fail. • When we add nodes the network gets more complex.
Mesh	• Redundancy. • There is no disruption when we add or remove nodes. • It can withstand high traffic.	• High cost. • The administration of the network is very complex.
Hybrid	• It can be modified according to our needs. • Large number of alternative data paths. • If a node fails the network can remain operational.	• High cost. • The administration of the network is very complex. • Very complicated to extend the network

3 Standards in Advanced Metering Infrastructure – Smart Metering

3.1 Smart Grid

Smart grid is one of the major trends and markets which involves the whole energy conversion from the supplier to consumer. There are many definitions about what smart grid is but the following is the most popular:

*"*an automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances." [13]

The role of smart grid is to give solutions in order to improve the energy value chain. This can lead to a better control and observation of the performance of the power system which can be achieved by sharing information between the different subsystems of the power system. Smart grid has a significant environmental impact which means that it can decrease the whole energy consumption of the electricity supply system.

3.2 Advanced Metering Infrastructure – AMI

Advanced metering infrastructure includes state-of-the-art hardware and software which measures and process interval data from the power system. This means that AMI is not a single technology but an integration of many technologies that can provide the appropriate connection between the consumer and the service provider. AMI gives to the users the ability to measure frequently in time-based and transmit this information to other parties in order to take decisions. Furthermore, AMI consists of various parts which are:

- Smart meters
- Wide-area communications infrastructure
- Home (local) area networks (HANs)
- Meter Data Management Systems (MDMS)
- Operational Gateways

During the past years, consumers had a passive role as users of the electricity and were charged accordingly to their use. Smart grid changed this scenario using the price of electricity as a motivator. As a result, consumers became more aware about the usage of electricity and AMI can help them to achieve this Smart Grid vision. This vision needs significantly larger efforts in order to have an integrated solution. This is the main reason why interoperability standards are needed in order to gain all the benefits from this technology. Figure 3.1 is a typical AMI interface. [14]

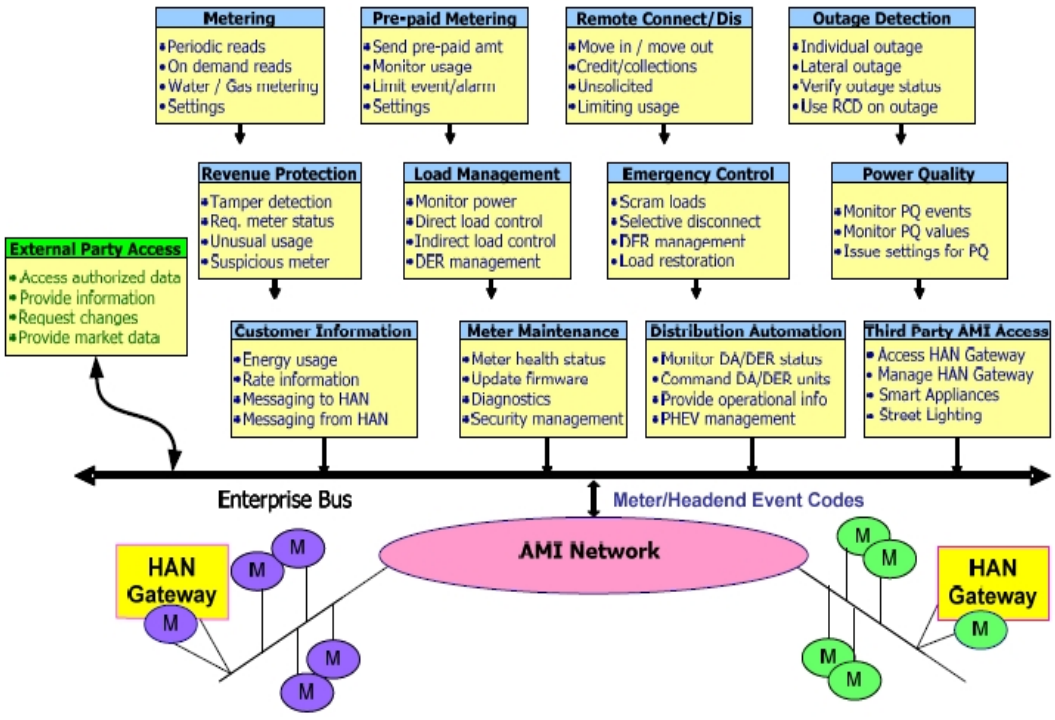

Figure 3.1 AMI interface [14]

Nowadays, vendors are developing systems according to their needs in order to meet specific utility requirements. As it was expected, every vendor developed its solution

according to its strengths. The problem begins when they want to exchange information with other vendor systems. If every vendor follows his own pattern then the exchange of information between them is impossible. This is the reason why vendors have to make external agreements on how these information exchanges will designed.

Moreover, the existence of a large group of vendors which have a large variety of products and systems leads to a Tower of Babel. Many parties have to come to discussion in order to agree in the development of a set of rules (standards) in order to achieve interoperability between different products and systems.

In order to have a clear view on the importance of these standards the following reasons can help us:

- Avoid reinventing the wheel
- The specification of requirements becomes easier
- Prevent the lock-in to a single vendor
- AMI can deployed in a much larger market

The challenge that smart grid technology faces today is not the lack of knowledge that is needed in order to solve this problem, but the need to solve the problem rapidly in order not to lose the faith, the loyalty and the public awareness or the momentum of the industry.

Before examining every standard in detail, it is very important to mention that the scale of an AMI network is similar to the Internet. Likewise Internet consists of millions of devices (i.e. laptops, desktops, mobile phones, etc.), AMI network consists of millions of consumers devices. The number of devices in an AMI network may be differ in the future because new devices may join this network. Figure 3.3 illustrates the components of a typical AMI system.

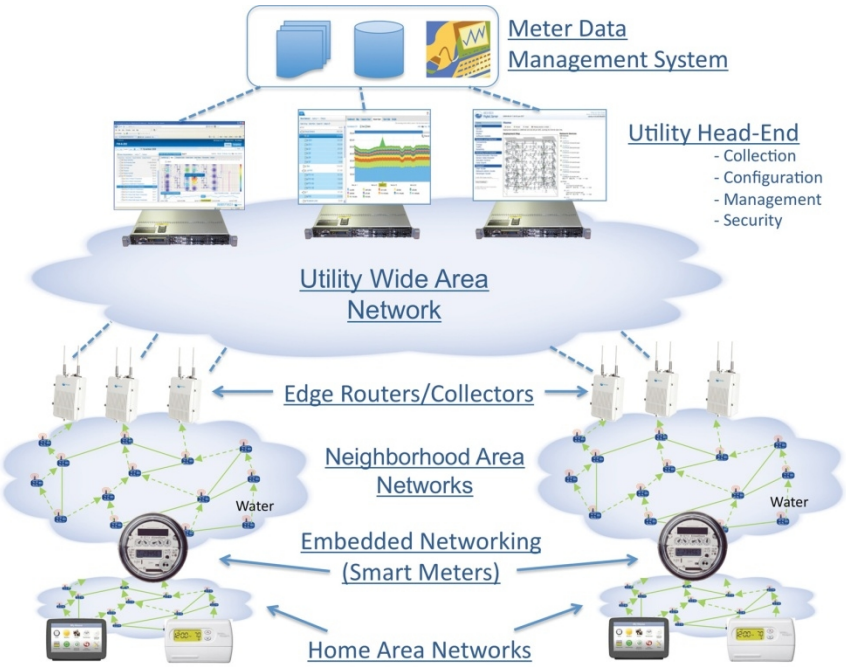

Figure 3.2 Components of an AMI system

The standards that developed for AMI are in fact the same IP standards that are used in the Internet. Moreover, the organizations that developing AMI standards are the same with the organizations that are involved in the development of the IP standards (i.e. IETF, IEEE, and W3C). There are organizations which haven't played an important role in the development of the IP standards but they are not irrelevant to the utility industry like IEC and UCAIug. Coordinator of these group's efforts is the NIST's Smart Grid Interoperability Panel (SGIP), with a process named as Priority Action Plans (PAPs) which addresses every critical gap in the development of AMI standards. Every organization has a role in the AMI standardization which is: [15]

- *NIST* is the National Institute of Standards and Technology (part of the Department of Commerce), which as it was said before, is the coordinator of the standardization efforts for the entire smart grid, with contributions from other organizations in their respective areas of expertise and focus.
- *IEEE*, is the Institute of Electrical and Electronics Engineers, is working to standardize the MAC and physical layers of wireless AMI networks.

- *IEC*, the International Electrotechnical Commission, is defining the common information models which can be used from AMI and smart grid.
- *IETF*, is the Internet Engineering Task Force, which is working to define the IP routing and adaptation layer protocols to enable efficient IP implementation over emerging link technologies from IEEE that are relevant to AMI networks.
- *W3C*, is the World Wide Web Consortium, is working to standardize the message formats for efficient data delivery over AMI networks.
- *UCAIug*, the Utility Communications Architecture International Users Group, has, through its OpenHAN working group, led the efforts to define the requirements for devices communicating over the HAN.
- *ZigBee Alliance* is an industry organization that has led the effort to define the Smart Energy Profile, a common information model for in-home control and display devices.

Figure 3.4 gives a summary view of the protocol layering of the AMI communications which are used in wireless mesh networks.

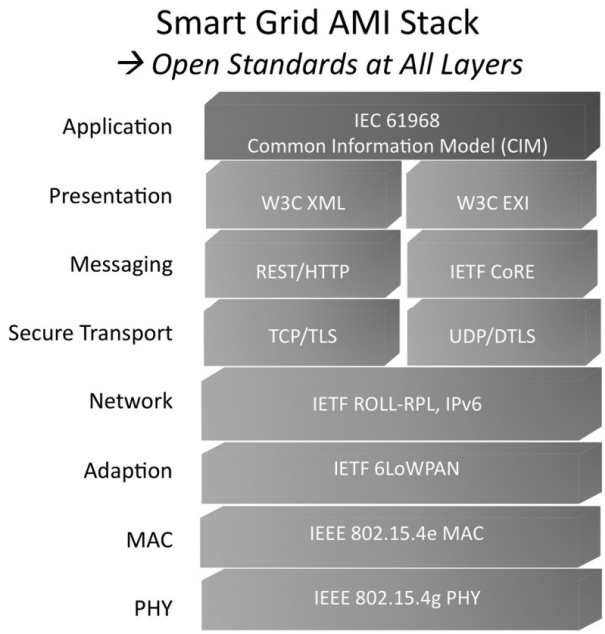

Figure 3.3 Standards in all layers of AMI

In the following paragraphs the most popular standards will be described in detail.

3.3 IEEE p2030

3.3.1 IEEE Organization

The IEEE is one of the leading developers of standards globally that underpin the most essential technologies. These technologies can belong in traditional fields (i.e. information technology, telecommunications, power and energy, transportation, medical and healthcare, etc.) or in emerging fields like nanotechnology. IEEE standards are recognized by the American National Standards Institute (ANSI) and until now nearly 1,300 standards are compelled or are under development.

Numerous IEEE standards related to the smart grid include diverse fields. These fields are: [16]

- Digital information and controls technology
- Networking
- Sensors
- Security
- Reliability assessment
- Interconnection of distributed resources including renewable energy sources to the grid
- Systems engineering
- Electric metering
- Broadband over power line

The standards are developed by a variety of expert groups within IEEE (Figure 3.5). [17]

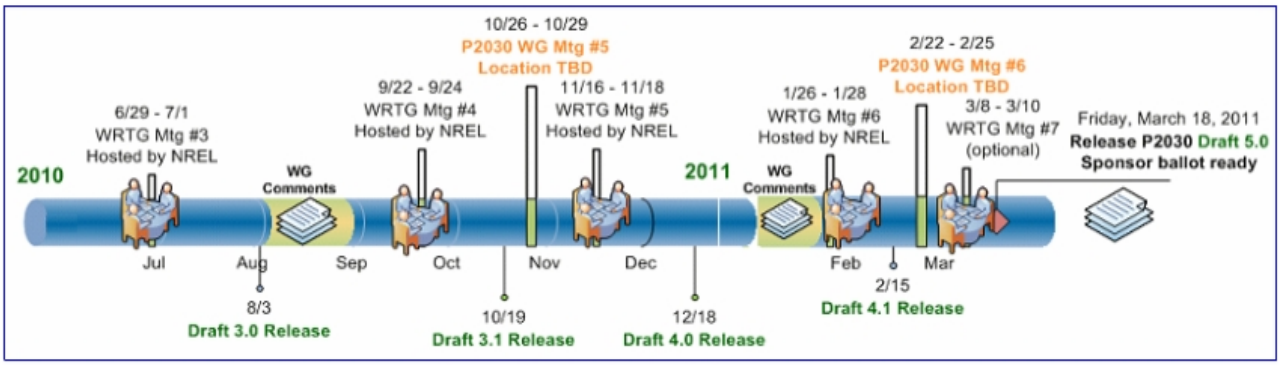

Figure 3.4 Roadmap of IEEE p2030 standard [18]

3.3.2 Description of IEEE p2030

The IEEE p2030 standard presents an interoperable design and implementation for systems that exchange information between smart grid elements, loads, and end-user applications. The IEEE p2030 standard, as we can see in the following image, is a conceptual representation of the smart grid architecture from three perspectives: power systems, communications and information technology (Figure 3.6). [19]

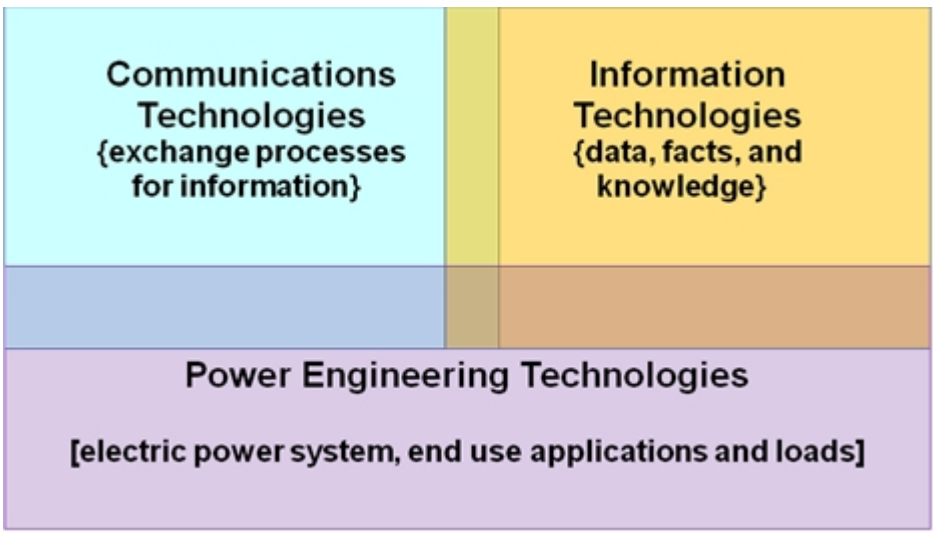

Figure 3.5 Perspectives of IEEE p2030 standard [19]

It presents a set of labeled diagrams that offer standards-based architectural direction for the integration of energy systems with information and communications technology infrastructures of the evolving Smart Grid. Furthermore its aim is to establish a common language for the smart grid community in order to communicate effectively.

The IEEE p2030 smart grid interoperability reference model (SGIRM) is a reference tool that can provide to stakeholders a common understanding of interoperability criteria from the perspectives of power system and the perspective of information and communications technology. Moreover, the IEEE p2030 SGIRM identifies and defines the interfaces between functional domains of the power grid from each of the perspectives and also describes the relationships among the domains, including the characteristics of the data that flow between them. Having this in mind, it is very easy to plan optimal design criteria for the interoperability of smart grid implementations. The goal of the IEEE p2030 SGIRM reference tool is to allow extensibility, scalability, and upgradeability. These principles, as well as other guiding principles that IEEE p2030 SGIRM follows, provide continuing evolution of the Smart Grid, increased functionality and innovation. The IEEE p2030 SGIRM consists of two components:

- Smart grid interoperability architectural perspectives (IAPs)
- Characteristics of the data that flows between the entities within these perspectives.

3.3.3 IEEE Standard p2030 series

Currently, there are three additional complementary standards designed to expand upon the base 2030 standard: [20]

- **IEEE P2030.1**, *Guide for Electric-Sourced Transportation Infrastructure* which is intended to establish guidelines that can be used by utilities, manufacturers, transportation providers, infrastructure developers and end users of electric-sourced vehicles and related support infrastructure in addressing applications for road-based personal and mass transportation.
- **IEEE P2030.2**, *Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure* which is intended to help users achieve greater understanding of energy storage systems by defining interoperability characteristics of various system topologies and to illustrate how discrete and hybrid systems may be successfully integrated with and used compatibly as part of the electric power infrastructure.

- **IEEE P2030.3**, *Standard for Test Procedures for Electric Energy Storage Equipment and Systems for Electric Power Systems Applications* which is intended to establish a standard for test procedures around verifying conformance of storage equipment and systems to storage interconnection standards.

IEEE Standard p2030.1

The guide for this standard addresses applications for electric-sourced vehicles and related support infrastructure used in road-based personal and mass transit. Furthermore, it provides a knowledge base addressing terminology, methods, equipment, and planning requirements for such transportation and its impacts on commercial and industrial systems. These guidelines can be used by transportation providers, infrastructure developers, manufacturers, end users of electric-sourced vehicles and also by related support infrastructure for road-based personal and mass transportation applications. This standard allows manufacturers to understand the requirements in order to implement the applications. As the supporting systems and methods are developed and standardized, IEEE p2030.1 allows end users to understand technologies that can be implemented for their transportation energy needs. This standard suggests a phased implementation and is based on economic considerations for technologies that are available today or are in development. Regional political facts or regulators may modify these methods, but this standard does not take under consideration the wide range of regional differences that exist.

IEEE Standard p2030.2

This standard provides guidelines for discrete and hybrid energy storage systems that exist in the electric power infrastructure, including end-user applications and loads. The purpose of IEEE p2030.2 is to provide guidance in understanding and defining technical characteristics of energy storage systems and how discrete or hybrid systems may be integrated with as part of the electric power infrastructure. Additionally, IEEE p2030.2 provides a knowledge base addressing terminology, evaluation criteria, operations, test-

ing, functional performance, and the application of engineering principles for energy storage systems integrated with the electric power infrastructure.

IEEE Standard p2030.3

Traditionally, utility electric power delivery systems were not designed to accommodate electric storage. Nowadays, electric storage has gained more and more attention as the development of renewable energy distributed resources interconnected with power systems has been deployed. This IEEE p2030.3 standard establishes test procedures for electric energy storage equipment and electric power systems (EPS) applications. Electric energy storage equipment or systems can be from a single device providing all required functions to an assembly of components, each of them having limited functions. Furthermore, requirements on installation, evaluation and periodic tests are included in this standard. Storage equipment and systems that are connected in an EPS must meet the requirements that are specified in IEEE p2030.3 until 2030. It is clear that test procedures are necessary in order to establish and verify compliance with those requirements. These test procedures need to provide repeatable results at independent test locations and also to have the appropriate flexibility in order to accommodate the variety of storage technologies and applications that exist.

3.4 TASE.2

The Inter Control Center Protocol (known as TASE.2 or IEC60870-6) is a protocol designed for communication between control centers within the energy industry, built on top of the Manufacturing Message Specification (MMS). TASE.2 was designed for bidirectional Wide Area Network (WAN) communication between a utility control center and other control centers, power plants, substations, and even other utilities. In this bidirectional communication a data exchange takes place which consists of real-time and historical power system monitoring and also control data which includes measured values, scheduling data, energy accounting data, and operator messages.

During the past years many custom and proprietary protocols were used by different vendors, as a result there was a need for a common protocol for standardized and reliable data exchange between control centers. Furthermore, it was important the designing of a protocol that could guarantee a reliable data exchange between control centers that are operated by different owners, produce different products, or perform different operations. Moreover, a standardized protocol becomes necessary in order to support the unique business and operational requirements of industry, especially in the case of the electrical utilities that require careful load balancing within a bulk system which is operated by many different facilities. [21]

In 1991, a working group was formed with a goal to develop and test a standardized protocol. This working group will then submit the specifications to the IEC. The initial protocol was called ELCOM-90, or Telecontrol Application Service Element-1 (TASE.1). TASE.1 evolved into TASE.2, which is the most commonly used form of ICCP.3. [22]

The design goals of TASE.2 were:

- higher safety of the plant
- lower costs of components
- reduced costs for installation and operating
- shorter times for planning, design and installation
- simplified selection of the devices and systems
- increasing interoperability
- lower training costs
- higher usage of the operating resources
- vendor independency
- more support by the supplier
- use of generally available industrial solutions.

3.4.1 Operations that TASE.2 can perform

TASE.2 is used to perform a number of communication functions between control centers, some of them are the following:

- Establishing a connection.
- Accessing information (read requests).
- Information transmission (such as e-mail messages or energy market information).
- Notifications of changes, alarms, or other exception conditions.
- Configuration of remote devices.
- Control of remote devices.
- Control of operating programs.

3.4.2 How TASE.2 works

The TASE.2 protocol establishes communication between two control centers using the client-server model. One control center is used as a server containing application data and defining functions. The other control center is used as a client sending requests to the server, then the server reads them and finally the server responds to these requests. Client initiated interactions are called "operations". Server initiated interactions are called "actions". These communications in TASE.2 have a common format so as to ensure interoperability. Four semantics are provided to exchange data between control centers: "once" (immediate client-server request), "periodic" (periodic transfer), "exception"(state change based transfer) and "event" (event condition based transfer). [22]

Operations that take place in the TASE.2 protocol can be seen in figure 3.7.

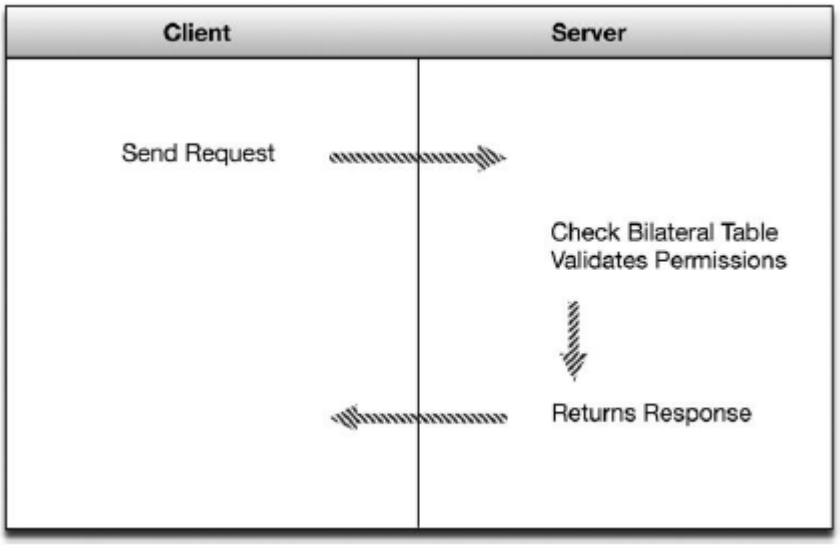

Figure 3.6 Operations in TASE.2 [22]

Although TASE.2 is mostly a unidirectional client-server protocol, there are modern implementations that support both functions, allowing a single TASE.2 device to operate as both a client and a server, and thus supporting bidirectional communication over a single connection.

Furthermore, TASE.2 has the ability to operate over any network protocol, including TCP-IP. This protocol is effectively a point-to-point protocol due to the fact that is using a "bilateral table" that explicitly defines an agreement between two control centers connected with an TASE.2 link, as it is shown in the previous image. The bilateral table is essentially an access control list that identifies in which data elements a client can have access.

The permissions defined within the bilateral tables in the server and the client are the authoritative control over what is accessible to each control center. Additionally, the entries in the bilateral tables must match on both the client and the server, in order to ensure that the permissions are agreed upon by both centers (remembering that TASE.2 is used to interconnect to other organizations in addition to internal WAN links to substations).

Access control is handled at the organization level between centers through a Bilateral Agreement. A bilateral agreement defines formally the set of data that are exchanged between control centers. It is the responsibility of servers to ensure access control. Data

structures are represented through Data Objects, and Data Value Objects which provide their values. Data Value Objects can be measurements (real or integer) or status (bit strings). Data Value Objects can have attributes (freshness, timestamp, way the data is provided etc.). Data Objects can be gathered in Data Set Objects.

3.4.3 Where TASE.2 is used

TASE.2 is widely used between control system enclaves and between distinct control centers. This standard must be understood as a tool box for any application domain with comparable requirements. For example, it can be used between two electric utilities, between two control systems within a single electric utility, between a main control center and a number of substations, etc. It provides a generic solution for advanced Information and Communication Technology. [22]

Figure 3.8 is a typical TASE.2 use within the Industrial Network environment.

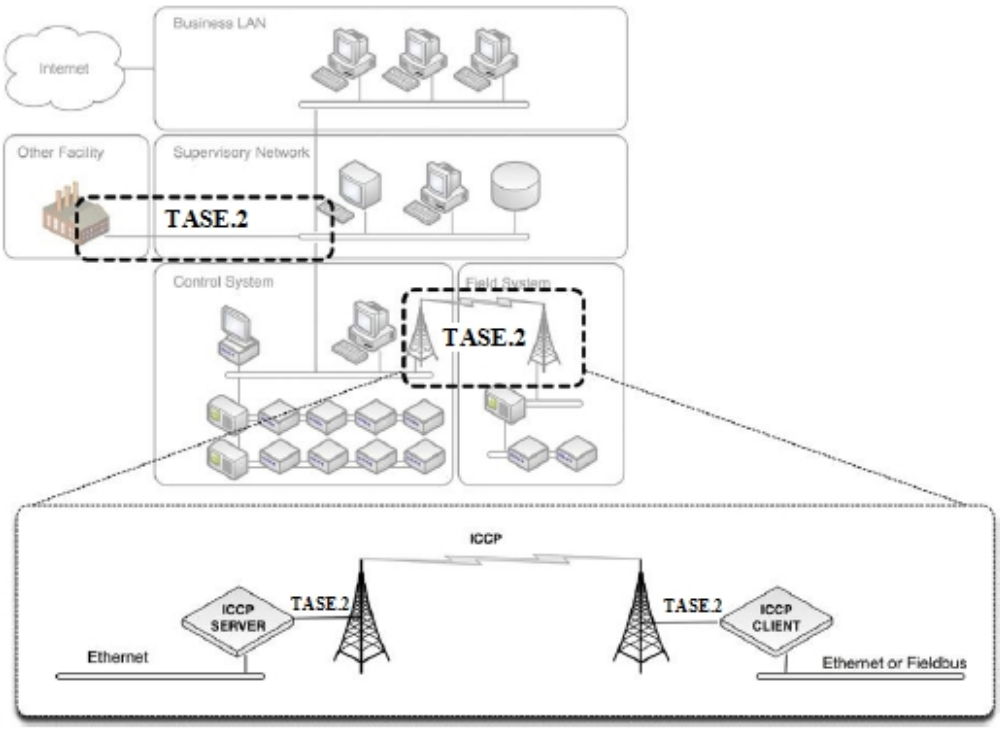

Figure 3.7 Typical TASE.2 example [22]

3.5 Power Line and IEC

3.5.1 Power Line Communication systems – Description

Communications over power lines (PLs) isn't something new but it dates back to the early 1900's. Power line communication systems (PLCs) were used by utility companies around the world for remote metering and load control, using at the beginning single carrier narrowband (NB) solutions operating in the Audio/Low Frequency bands that achieved data rates ranging from few bps to a few kbps. The advantage of using these systems is that every home and general every building is equipped with power line as a result there is no need for new infrastructure. PLC systems are using the power line wiring as a medium for the communication which in most cases is more reliable and secure. Furthermore, PLC has moved from the experimental phase and now it is mature enough so as to use it in AMI applications (Figure 3.9). [23]

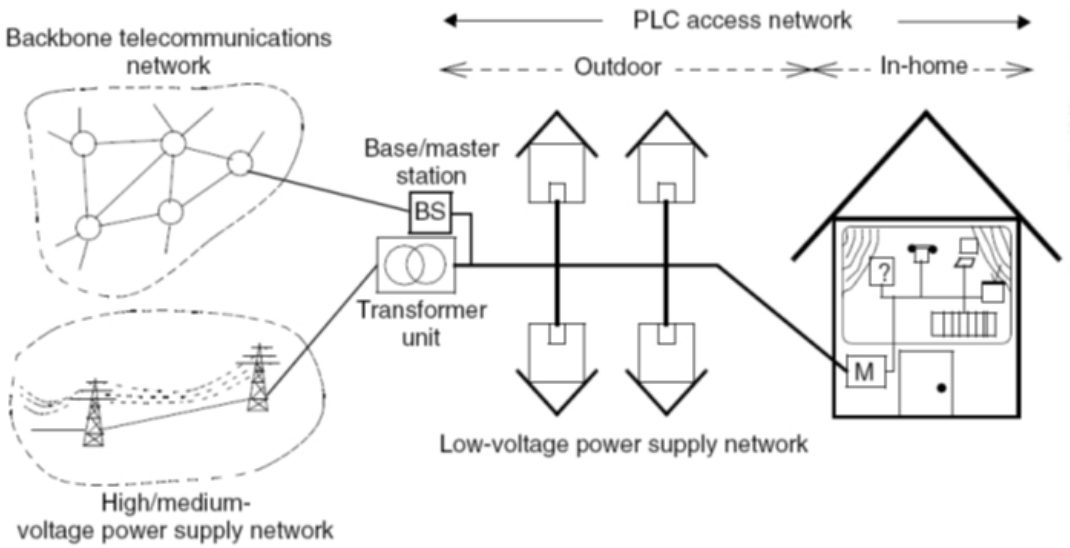

Figure 3.8 Example of a PLC system

A new era began when the technology matured and the application space widened. Broadband (BB) PLC systems operating in the High Frequency band (2-30 MHz) appeared in the market and these systems could achieve data rates up to a 200 Mbps. Nowadays, industry interest has focus in high data rate NB PLC systems which are based on multicarrier schemes and operating in the band between 3-500 kHz.

3.5.2 Classes of PLC systems

Ultra Narrow Band (UNB): Systems operating at very low data rate (approximately 100 bps) in the Ultra Low Frequency (0.3-3 kHz) band or in the upper part of the Super Low Frequency (30-300 Hz) band. A previous example of a one-way communication link supporting load control applications is Ripple Carrier Signaling, which operates in the 125 - 2,000 kHz and is able to convey several bps band using simple Amplitude Shift Keying modulation. More recent examples are the AMR Turtle System, which conveys data at extremely low speed (~0.001 bps) and the Two-Way Automatic Communications System (TWACS), which can carry data at a maximum data rate of two bits per mains frequency cycle, i.e. 100 bps in Europe and 120 bps in North America. UNB-PLC has a very large operational range (150 km or more). Although the data rate per link is low, deployed systems use various forms of parallelization and efficient addressing that support good scalability capabilities. Despite the fact that these UNB solutions are proprietary, they are very mature technologies, they have been in the field for at least two decades, and have been deployed by hundreds of utilities. [23]

Narrowband (NB): Systems operating in the VLF/LF/MF bands (3-500 kHz), which include the European CENELEC (Comite´ Europe´en de Normalisation Électrotechnique) bands (3-148.5 kHz), the US FCC (Federal Communications Commission) band (10-490 kHz), the Japanese ARIB (Association of Radio Industries and Businesses) band (10-450 kHz), and the Chinese band (3-500 kHz). Specifically, we have:

Low Data Rate (LDR): Single carrier systems capable of data rates of few kbps. Typical examples of LDR NB-PLC systems are devices conforming to the following recommendations: ISO/IEC 14908-3 (LonWorks), ISO/IEC 14543-3-5 (KNX), CEA-600.31 (CEBus), IEC 61334-3-1, IEC 61334-5 (FSK and Spread-FSK), etc. Additional non-SDO based examples are Insteon, X10, and HomePlug C&C, SITRED, Ariane Controls, BacNet etc.

High Data Rate (HDR): Multicarrier systems capable of data rates ranging between tens of kbps and up to 500 kbps. Typical examples of HDR NB-PLC systems are devices

within the scope of ongoing standards projects: ITU-T G.hnem, IEEE 1901.2. Additional non-SDO based examples are PRIME and G3-PLC. [23]

Broadband (BB): Systems operating in the HF/VHF bands (1.8-250 MHz) and having a PHY rate ranging from several Mbps to several hundred Mbps. Typical examples of BB-PLC technologies are devices conforming to the TIA-1113 (HomePlug 1.0), IEEE 1901, ITU-T G.hn (G.9960/G.9961) recommendations. Additional non-SDO based examples are HomePlug AV/Extended, HomePlug Green PHY, HD-PLC, UPA Powermax, and Gigle MediaXtreme. [23]

3.5.3 PLC standardization

The biggest problem that PLC technology faces is the standardization status. During the last three years, we were moved from a complete lack of any standard in PLC systems to the opposite phenomenon of having multiple non-interoperable standards from different organizations. This leads to confusion in the PLC market on which standard should be followed. In the following paragraphs every standardization organization and the most important standards will be described. [24]

Standardization Organizations and Research Groups

The most important organizations and research groups that created standards for the PLC technology in AMI are the following: [24]

European Telecommunications Standards Institute (ETSI) power-line telecommunications (PLT): this project provides a necessary standards and specifications for voice and data services over the power line transmission and distribution network and/or in-building electricity wiring. The standard discusses interoperability aspects between equipment from different manufacturers and co-existence of multiple power-line systems within the same environment.

Home-Plug Power-Line Alliance: The Home Plug Power-Line Alliance is a global organization consisting of 65 member companies. Their mission is to enable and promote rapid availability, adoption and implementation of cost effective, interoperable and standards-based home power-line networks and products. Because Home Plug technology is based on the contributions of multiple companies from around the world, the re-

sulting standards are expected to offer best performance. The Home Plug Power-Line Alliance has defined some standards like:

- Home Plug 1.0. Specification for connecting devices via power-lines in the home.
- Home Plug AV. *D*esigned for transmitting high definition television (HDTV) and VoIP around the home.
- Home Plug BPL. A working group to develop a specification for to-the-home connection.
- Home Plug Command and Control (CC). Command and control a specification to enable advanced, whole-house control of lighting, appliances, climate control, security and other devices.

Institute of Electrical and Electronics Engineers (IEEE): the standards are due to the IEEE BPL Study Group. Some of those standards are:

- IEEE P167*:* "Standard for Broadband over Power-line Hardware" is a working group working on hardware installation and safety issues.
- IEEE P1775: "Power-Line Communication Equipment – Electromagnetic Compatibility (EMC) Requirements – Testing and Measurement Methods" is a working group focused on PLC equipment, EMC requirements and testing and measurement methods.
- IEEE P1901: "IEEE P1901 Draft Standard for Broadband over Power-Line (BPL) Networks: Medium Access Control and Physical Layer Specifications" is a working group for delivering BPL. The aim is to define medium access control and physical layer specifications for all classes of BPL devices from long distance connections to those within subscriber premises.

POWERNET: Powernet is a research and development project with funding from the European Commission. It aims at developing and validating a 'plug and play' cognitive broadband over power-lines (CBPL) communications equipment that meet the regulatory requirements concerning electromagnetic radiations and can deliver high data rates while using low transmit power spectral density and working at low signal-to-noise ratio.

Open PLC European Research Alliance: Open PLC European Research Alliance (OPERA) is a research and development project with funding from the European Commission. It aims at improving/developing PLC services and system standardization.

Universal Power-Line Association (UPA): The UPA aligns industry leaders in the global PLC market to ensure deployment of interoperable and coexisting PLC products to the benefit of consumers worldwide.

Most Important PLC Standards

The IEEE 1901 Standard

The IEEE P1901 Working Group was established in 2005 to unify power line technologies with the goal of developing a standard for high-speed (> 100 Mb/s) communication devices, using frequencies below 100 MHz and addressing both HN and access applications. A baseline of the standard passed the confirmation vote in December 2008 and defines three PLC technologies: an FFT-OFDM-based PHY/MAC, a Wavelet-OFDM-based PHY/MAC and a G.9960 Compatible PHY/MAC. As per the scope of IEEE 1901, the standard will be usable by all classes of PLC device, including those used for the first-mile/last-mile (<1500 m to the premise) broadband services as well as devices used inside buildings for Local Area Networks (LANs) and other data distribution (<100 m between devices) applications. The FFT-OFDM 1901 PIIY specification facilitates backward compatibility with devices based on the HomePlug AV industry specification. Similarly, the Wavelet-OFDM 1901 PHY specification facilitates backwards compatibility with devices based on the I ID-PLC Alliance industry specification. [25]

The ITU-T G.9960 Standard

The ITU-T started the 'G.hn' project in 2006 with a goal of developing a worldwide recommendation for a next generation unified home network transceiver, capable of operating over all types of in-home wiring: phone lines, power lines, coax and Cat 5 cables and bit rates up to 1 Gbps. In December 2008, ITU-T consented on Recommendation G.9960, which is the G.hn foundation and specifics system architecture, most of the PHY and data-path related parts of the MAC. The technology targets residential houses and public places, such as small/home offices, multiple dwelling units or hotels. G.9960 did not originally address PLC Access and Smart Grid applications, but in mid 2009 a proposal for addressing Smart Grid applications was approved by the group. Further-

more, coexistence mechanisms with 1901 IH and access devices are currently under study.

G.9960 allows up to 250 nodes operating in the network. It defines several Profiles to address applications with significantly different implementation complexity. High-profile devices, such as residential gateways, are capable of providing very high throughput and sophisticated management functions. Low-profile devices, such as home automation or Smart Grid applications, have low throughput and only basic management functions, but they can interoperate with higher profiles.

Past approaches emphasized transceiver optimization for a single medium only, i.e. either for power lines, phone lines or coax cables. The approach chosen for G.9960 is a single transceiver optimized for multiple media. Thus, G.9960 transceivers arc parameterized so that relevant parameters can be set, depending on the wiring type. For example, a basic multicarrier scheme based on windowed OFDM has been chosen for all media, but some OFDM parameters, such as number of subcarriers and subcarrier spacing, are media dependent. Similarly, a three-section preamble is defined for all media, but durations of these sections change on a per media basis. A quasi-cyclic LDPC (QC-LDPC) code has been chosen for FEC, but a particular set of coding rates and block sizes are defined for each type of media. A parameterized approach also allows to some extent optimization on a per media basis to address channel characteristics of different wiring without sacrificing modularity, flexibility and cost. [25]

3.5.4 Problems that exist in PLC technology

PLC technology is widely used for AMI applications but some problems still exist. Moreover, if we want to support the exclusive use of the PLC technology for AMI applications then a big question rises of which standard should we follow and how compatible with other systems can it be. This problem leads to confusion in the market and as a result deployments are delayed.

Another significant problem is the interference that exists between non-interoperable devices. Fortunately, there are standardized mechanisms which can limit this problem and make PLC systems efficient. These standardizes mechanisms are called “coexistence mechanisms”. Widely known is the PHY/MAC-agnostic coexistence scheme

CENELEC EN 50065 which allowed the ratification of several NB-PLC standards after its publication in 1992. [23]

3.5.5 IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes international standards for all electrical, electronic, and related technologies, primarily for the electric power industry, although some electrical ‐ related work in industrial processes is also undertaken.

The IEC Council consists of National Committees, one from each country which is a member of the IEC. Under the IEC Council are Standards Management Boards (SMBs) which coordinate the international standards work. This standards work is performed through the many Technical Councils (TCs), each tasked with specific areas. For instance, TC 57 is tasked to develop standards for communications and interoperability, and is home to the Working Groups (WGs) which are developing many of the Smart Grid interoperability standards.

These Working Groups consist of Technical Experts authorized by their National Committee to participate in the two to four meetings per year, in addition to undertaking significant work between meetings.

In the US, the National Committee is sponsored by ANSI. All voting on IEC standards is done by the National Committees. A typical timeframe for developing a new standard is approximately three to five years. A proposed standard starts as a Working Document (WD) developed in the Working Group, then is sent to all National Committees for review as a Committee Draft (CD), next resent to the National Committees for review and vote as a Committee Draft for Vote (CDV), then finally issued as an International Standard (IS), which is made available for purchase on the IEC web site. [14]

IEC TC 57 has developed specialized communications standards for the power industry, with on ‐ going work to expand and enhance these standards, which include:

- IEC 61850 for substation automation, distributed generation (photovoltaics, wind power, fuel cells, etc.), SCADA communications, and distribution automation. Work is commencing on Plug ‐ in Hybrid Electric Vehicles (PHEV).

- IEC 61968 for distribution management and AMI back office interfaces.
- IEC 61970 (CIM) for transmission and distribution abstract modeling.
- IEC 62351 for security, focused on IEC protocols, Network and System management, and Role‐Based Access Control.

IEC TC 13 handles metering and may undertake a joint effort with TC57 to work on communications for metering, specifically for AMI.

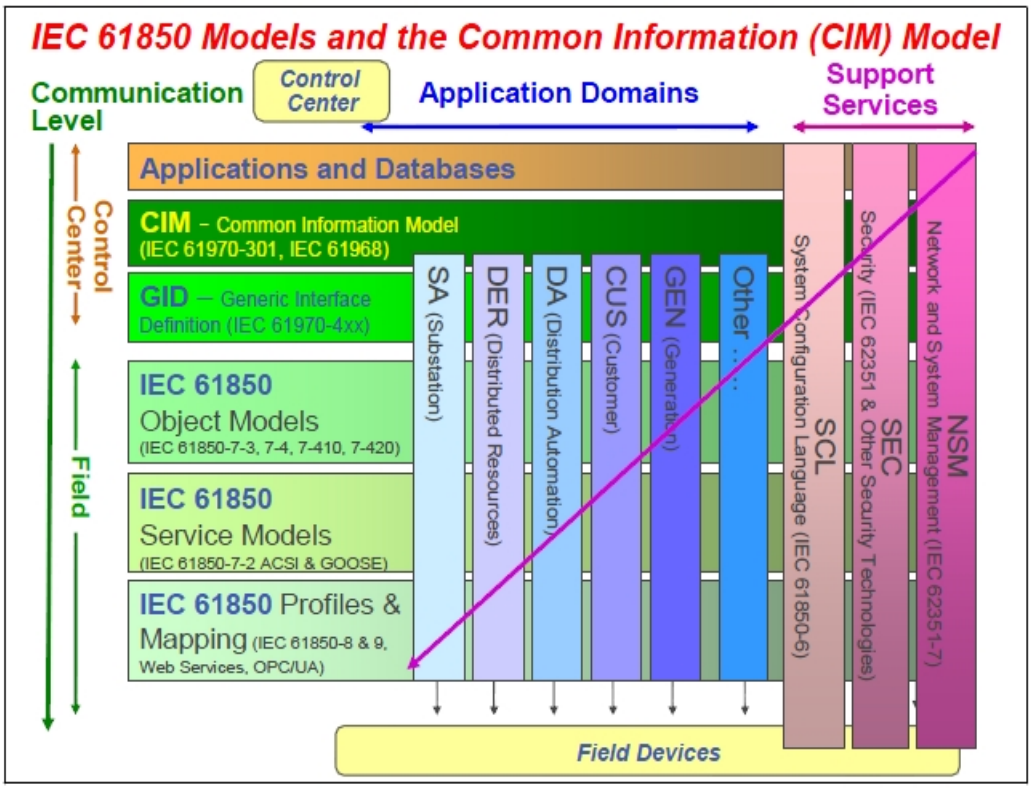

Figure 3.9 IEC 61850 models [14]

3.6 Other Standards

3.6.1 IEEE 802.15.4g Smart Utility Network (SUN)

IEEE 802.15.4g Task group was formed in order to promote open standards for Smart Grid environment and to meet the specific regional and national regulations in a global Smart Grid deployment environment in a scalable and cost-effective way. This Task Group, also known as the Smart Utility Networks (SUN) Task Group, had as a goal to

review the IEEE 802.15.4-2006 standards and to propose amendments principally for outdoor low data rate, wireless, smart metering utility networks. [26]

The implementation of IEEE 802.15.4g can be seen in figure 3.11.

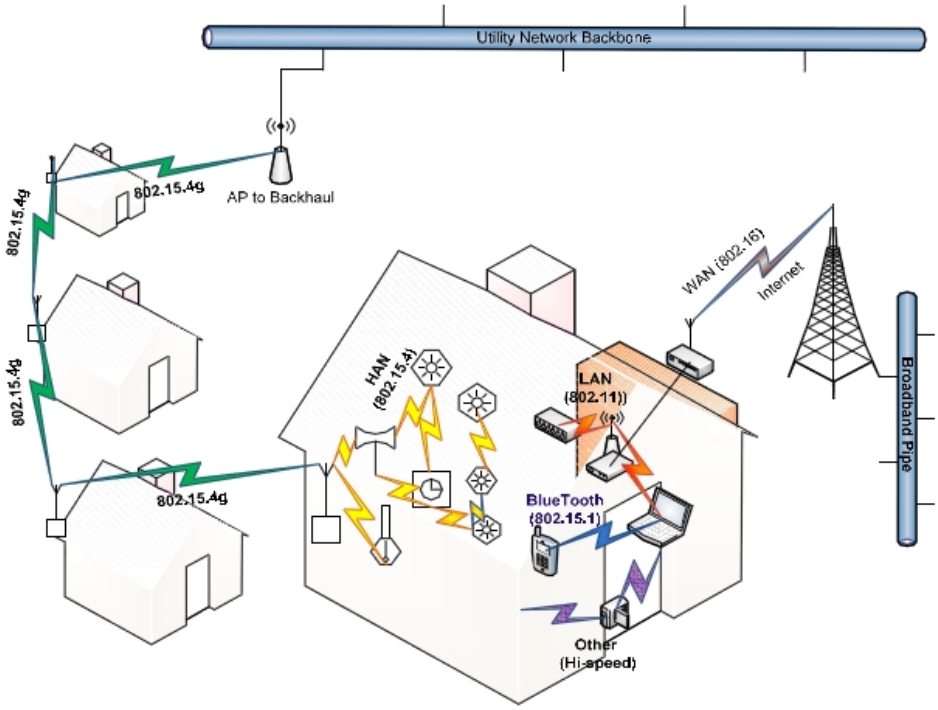

Figure 3.10 Implementation of IEEE 802.15.4g [18]

IEEE 802.15.4g is currently under ballot, meaning the draft of the full standard is stable and the IEEE imperative principle of consensus has to be found between voters and all comments addressed before 15.4g can be officially published. In addition to the new PHY, the amendment also defines MAC modifications (may also require 15.4e add-on features) needed to support their implementation. The SUN PHY supports multiple data rates in bands ranging from 450MHz to 2450 MHz and working in one of these 3 modes:

- Orthogonal frequency division multiplexing (MR-OFDM) PHY - provides higher data rates at higher spectral efficiency
- Multi-rate and multi-regional offset quadrature phase-shift keying (MR-O-QPSK) PHY - shares the characteristics of the IEEE 802.15.4-2006 O-QPSK PHY, making multi-mode systems more cost effective and easier to design.

- Multi-rate and multi-regional frequency shift keying (MR-FSK) PHY - good transmit power efficiency due to the constant envelope of the transmit signal.

IEEE 802.15.4g addresses regional regulations (i.e. North America, Europe, Japan, Korea and China) by adding support for new frequencies including sub-GHz frequency bands. The IEEE 802.15.4 radio can now operate in one of the dedicated use or unlicensed bands. Given that three PHYs are defined within the application space, it is possible that multiple, different SUN PHYs can be operating in the same location and within the same frequency band. In order to mitigate interference, a multi-PHY management (MPM) scheme is specified for SUN networks to enable inter-PHY coexistence. With the publication of IEEE 802.15.4-2011 specifications, a new and open ecosystem for large volume of standards-based semiconductors, including management tools, protocol analyzers and diagnostics tools can appear, helping to lower the cost of scaling up Smart Grid deployments worldwide. However, frequency bands in some region still needs to get harmonized for real success such as the on-going effort from the European Conference of Postal and Telecommunications Administrations (CEPT) to allocate new frequency bands (870-876MHz and 915-921MHz) in Europe.

Key industry players, i.e. Elster, Itron, Landis+Gyr, NICT, and Silver Spring Networks, had an active role in shaping the standard, striving to ensure backward compatibility with existing deployed devices, and ensuring that features necessary for long-term operation were represented. A significant, internationally recognized ecosystem contributed to the development of the standard including smart grid platform providers, equipment vendors, silicon suppliers, electric and gas utilities, and regulatory agencies. The standard is already supported by products from a large number of global vendors and is expected to rapidly gain worldwide adoption.

3.6.2 ANSI C.12 series

The American National Standards Institute (ANSI) has provided a standard metering protocol for many years. The C12 series of standards ensures interoperability between meter vendors by describing common data structures for typical meter exchanges (for example the collection of interval energy data). The protocol has been extended to pro-

vide remote meter reading over a range of communications links and most recently over IP connections.

Specifically, getting a large amount of meter data and configuring large volumes of meters was still considered a novel concept. Industry partners developed two ANSI protocol standards, ANSI C12.18 and ANSI C12.21 to facilitate deployment of multi-vendor solutions by utilities. Both standards use a session-based protocol, the Protocol Specification for Electricity Metering, or PSEM, and a physical connection, the ANSI Type 2 Optical Port and any serial connection, respectively. [27]

At its core, the C12.22 standard defines two things: a transport independent application level protocol for exchanging data between nodes, and a physical and data link protocol for linking meters. Like the C12.18 and C12.21 standards, C12.22 is designed to move C12.19 table data using PSEM messages.

PSEM, as defined by ANSI C12.18 and ANSI C12.21, is a session-based protocol wherein both parties to the communications are able to issue requests and responses. In some cases, the responses are mandatory, and lost responses may result in a reset of the communications link.

C12.22 extends PSEM with EPSEM, or the extended protocol specification for electronic metering. EPSEM adds the ability to chain commands, as well as several new commands for managing communications over a shared media with multiple nodes. In the following image we can see an example of the communication between a computer and a meter using C.12.22.

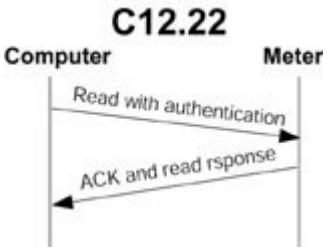

Figure 3.11 Communication between a computer and a meter in C12.22

C12.19 and C12.22 can be implemented on devices with relatively small amounts of microcode and processing power, including machines with as little as 64k of code space. This is important to consider when the scope of a full system roll-out of residen-

tial meters may involve millions of devices. Protocols with greater overhead or processing power needs may not be cost effective for general deployment.

3.6.3 DLMS/COSEM

The Device Language Message Specification (DLMS) and Companion Specification for Energy Metering (COSEM) form together the DLMS/COSEM application layer communication protocol and an interface model for metering applications. The DLMS-protocol enables the integration of energy meters with data management systems from other manufacturers. This secures that the energy supplier gets the full advantage of the meter functions. Using the wrapper layer defined in, DLMS/COSEM can be used over TCP/IP and UDP/IP. [28]

DLMS/COSEM is based on a strict client-server structure. The server is meant to be within the meter while the client accessing the meter could be a gateway or the central office. Other use cases where the server is within the gateway and the client is in the central office are also feasible.

The DLMS/COSEM specification follows a three-step approach as it is illustrated in figure 3.13: [29]

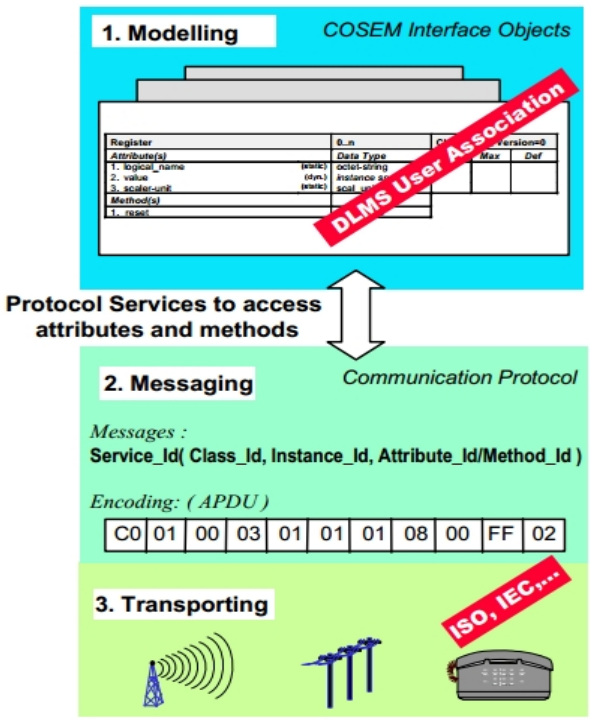

Figure 3.12 DLMS/COSEM specifications [29]

- Modeling: This covers the interface model of metering equipment and rules for data identification.
- Messaging: This covers the services for mapping the interface model to protocol data units (APDU) and the encoding of these APDUs.
- Transporting: This covers the transportation of the messages through the communication channel

Data exchange between data collection systems and metering equipment using the COSEM interface object model is based on the client/server paradigm. Metering equipment plays the role of the server. The data collection application and the metering application are modeled as one or more application processes (APs). Therefore, in this environment communication takes place always between a client and a server AP: the client AP requests services and the server AP provides them.

A client AP may be able to exchange data with a single or with multiple server APs at the same time. A server AP may be able to exchange data with one or more client APs at the same time. Furthermore, data exchange between server APs may be possible. Similarly, data exchange between client APs hosted by a single or multiple physical devices may be possible.

Data exchange takes place via exchanging messages (SERVICE.requests / .responses) between the two APs. In general, the client and the server APs are located in separate devices. Therefore exchanging messages is done via a protocol stack, or communication profile, as shown in figure 3.14:

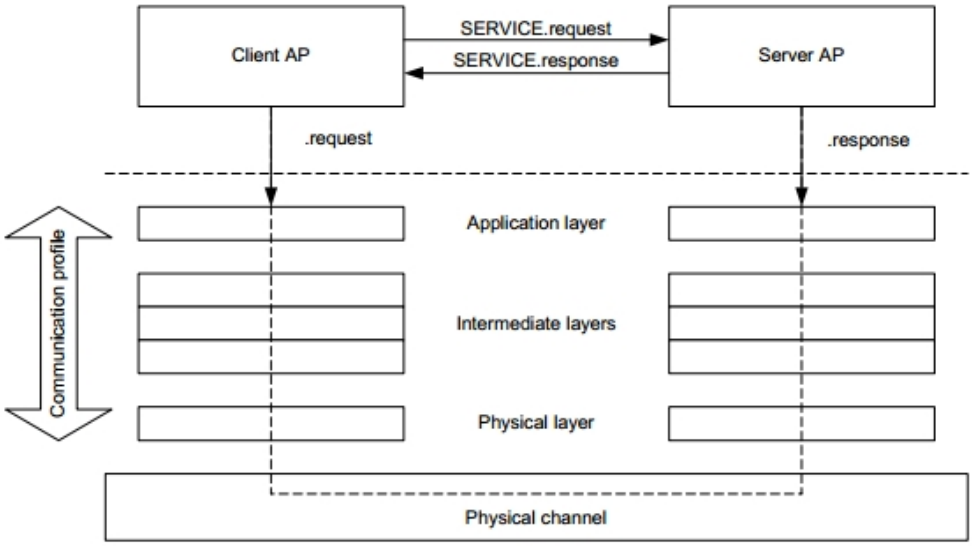

Figure 3.13 Message exchanging in DLMS/COSEM protocol [29]

Communication profiles comprise a number of protocol layers. Each layer has a distinct task and provides services to its upper layer and uses services of its supporting layer(s).

DLMS/COSEM supports clock synchronization and transmission of measurement profiles. So far DLMS/COSEM as standardized neither supports the transmission of digital signatures with measurement data nor a firmware download. Both will be supported in the future. Support for digital signatures is being worked on by the DLMS User Association. DLMS/COSEM includes authentication and confidentiality services based on symmetric encryption.

4 Networking an area with RF Mesh

This chapter investigates the performance of a mesh network where multiple sensors send their measurements to a server. Moreover, several experiments revealed problems that occur in a network that uses RF mesh protocols. The results of these experiments were taken under consideration during the implementation of a RF mesh protocol which tries to eliminate or to drastically reduce the problems that were discovered.

4.1 Sensors

In the experiments that will follow, several sensors were connected wirelessly with one goal which was to broadcast or to send packets to a specific destination. The type of the sensor that was used for these experiments is called “Jeenode”. This sensor is a small micro-controller board which can be used for a variety of Physical Computing tasks, from measuring things like temperature, humidity and other environmental data to tracking controlling energy consumption around the home area. The programming language that Jeenode uses is C or C++. Image 4.1 shows a Jeenode sensor.

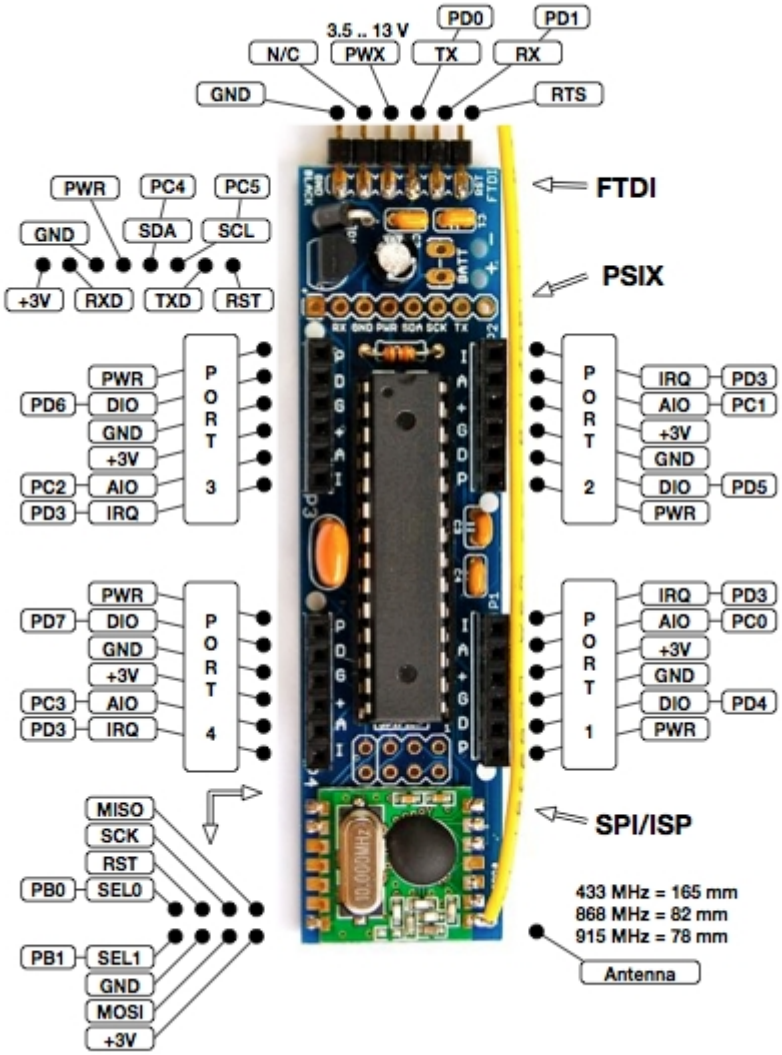

Figure 4.1 Jeenode Sensor

4.1.1 Components of the Jeenode Sensor

The components of a Jeenode sensor from the top to the bottom are:

- 6-pin FTDI-compatible serial I/O port
- 3.3V power regulator which accepts 3.5 to 13V as external power source
- 6-pin combined Power/Serial/I2C connector
- ATmega328 MPU by Atmel, with 16 MHz ceramic resonator
- 2x4-pin combined SPI/ISP connector, with 2 select lines
- RFM12B wireless RF module for the 433, 868, or 915 MHz ISM band, by Hope RF

- Two I/O "ports" each, with 1 analog/digital I/O, 1 digital I/O, +3.3V, ground, PWR, and interrupt (IRQ) line on both long sides of the board. All four ports have an identical pinout.

Image 4.2 illustrates a Jeenode sensor that isn't assembled with all the parts that is needed.

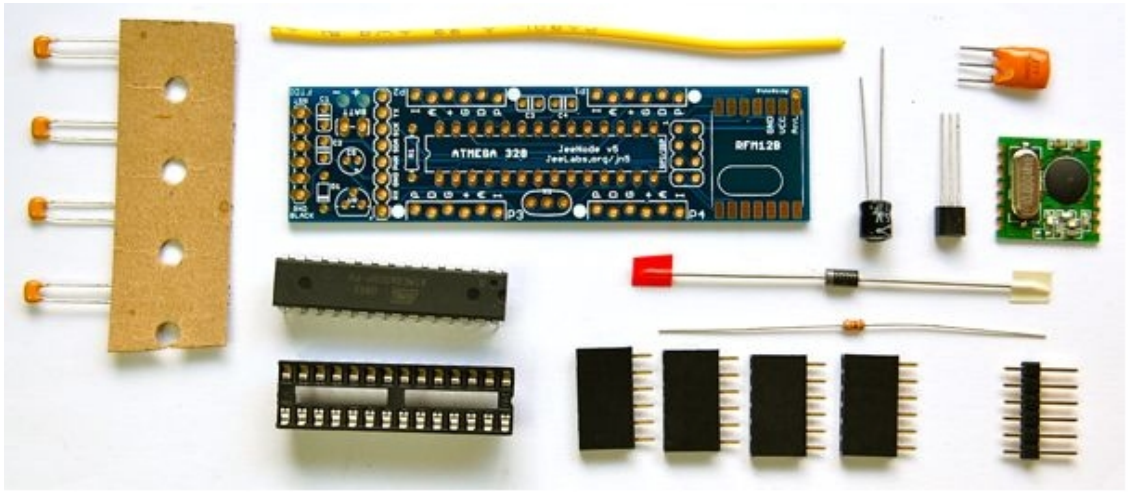

Figure 4.2 Parts of a Jeenode Sensor

The sensors that were used for this Dissertation were assembled by the IT department of International Hellenic University and me.

Figure 4.3 Assembly of a Jeenode Sensor

Furthermore, the wired antenna that was used during the experimentation phase had length of 82 mm in order the sensor to be able to operate in 868 MHz.

4.1.2 Supporting software for Jeenode

Jeenodes are very similar to Arduino boards and as a result they can use the same IDE as them. The Arduino IDE can run equally well on Widows, MAC or Linux. Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software.

Furthermore, Arduino IDE can sense the environment by receiving input from a variety of sensors and afterwards it can take decisions for the surroundings i.e. controlling lights, motors, and other actuators. The microcontroller on the board is programmed using the Arduino programming language (based on Wiring) and the Arduino development environment (based on Processing). All Arduino projects can be stand-alone or they can communicate with other software running on PC (e.g. Flash, Processing, MaxMSP).

The GUI of the Arduino IDE is shown in image 4.4.

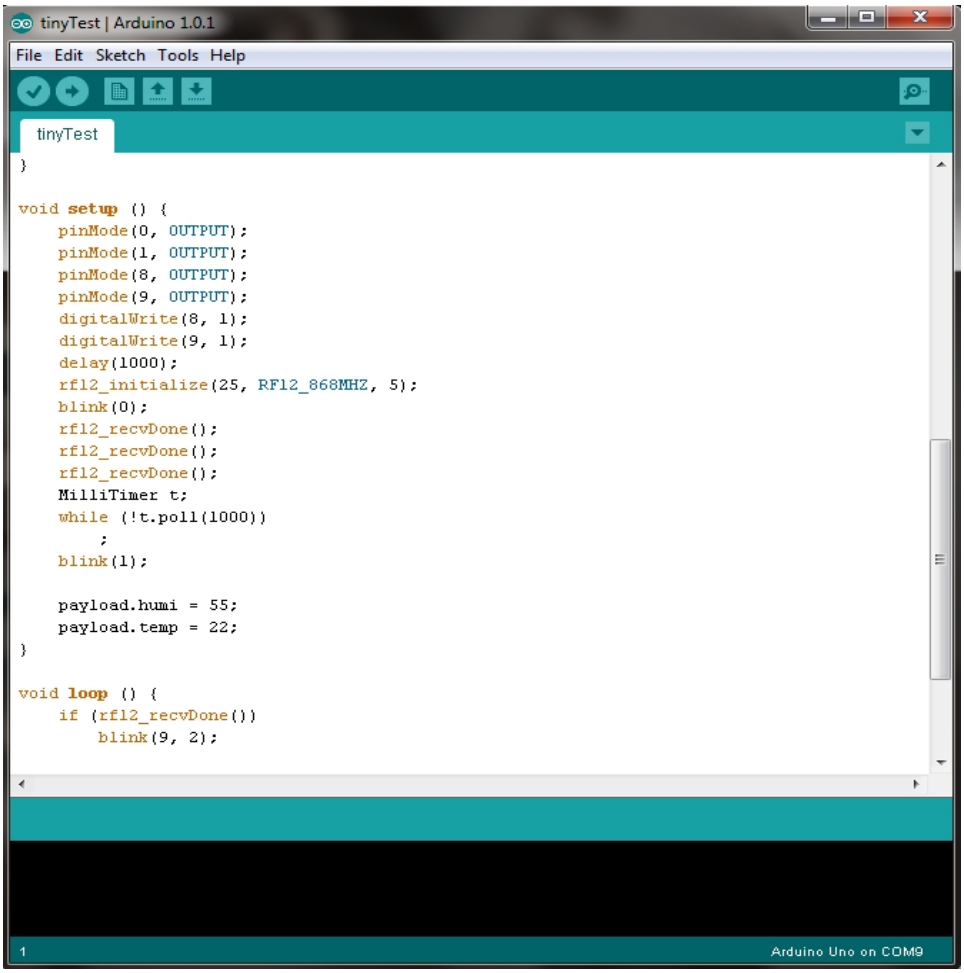

Figure 4.4 GUI of Arduino

The libraries that were added to Arduino IDE for better support of Jeenode are the following:

- The "Ports" library for an easy connection between a sensor and a specific port, and to re-load the same code when there is need of re-connecting those sensors to a different port later on. Moreover, it contains a few extras over what the standard Arduino / Wiring code offers: a bit-banging TWI driver which can run on any port (even on all of them in parallel) and simple shift functions to drive SPI-like devices.
- The "RF12" library contains a driver for the RFM12B module. It makes it easy to send packets of up to 66 bytes of data, either as broadcasts or in point-to-point mode. Furthermore, this library set ups a more reliable communication through the support of acknowledgements and retransmissions to deal with packet errors and losses.

4.2 Investigate performance

In order to investigate the performance of these sensors but also to found out the maximum range of correct reception, a series of experiments took place in International Hellenic University. These experiments can be divided into two categories, outdoor and indoor.

Furthermore, all sensors were operating in 868 MHz because in all other frequencies (433 or 915 MHz) the antenna wire should have different length. One sensor was the server who received packets from two other nodes. Moreover, the size of the packets in every experiment wasn't the same. In the beginning of every experiment the size of every packet had length of 6 data bytes and afterwards the length of every packet changed to 66 data bytes.

4.2.1 Outdoor environment

In the first experiment one sensor was transmitting 6 data bytes to another sensor who was the server. The maximum range in which the communication was reliable was 139 meters and after this distance there was no reception from the server.

Figure 4.5 Range of reliable communication (6 bytes)

Furthermore, in the next phase of this experiment, one more sensor was added in the same frequency band. As a result, the range that these two sensors could transmit simultaneously was decreased to 129 meters. In the distance of 133 meters, the server was receiving serial the packets from the two sensors and there wasn't a case that it received simultaneously a packet. Moreover, in the final phase of this experiment, the server could "hear" only one sensor in the distance of 138 meters.

The length of the packet in the second experiment was the attribute that was changed. The data bytes were increased from 6 bytes to 66 bytes in order to investigate if the data length would decrease the range of reception. In the beginning only one sensor was transmitting the data to another sensor who was the server. The maximum range of transmission and correct reception was 122 meters.

Figure 4.6 Range of reliable communication (66 bytes)

Thereafter, one more sensor was added in this network and the range that there was a simultaneously reception from the server was 101 meters. Furthermore, in the distance of 120 meters the server could receive serial the packets from the two sensors.

Simulation results

The results of the first experiment showed that the range of transmission using one transmitter and one receiver is 139 meters. The environmental conditions were tried to be similar to a "free space" but this is an imaginary scenario. The findings from the previous paragraphs will be compared with a free space propagation model.

The free space loss (FSL) is defined as: [30]

$$FSL = 32.5 + 20 \times \log_{10}(R) + 20 \times \log_{10}(F)$$

where R is the distance between the transmitter and the receiver in kilometers and F the frequency in MHz.

As a result the received power is equal to: [30]

$$P_R = P_T - FSL$$

The power of transmission of a Jeenode sensor, which was used in all series of experiments, is equal to 4 dBm and the receiver sensitivity is equal to -105 dBm. Image 4.7 shows a diagram where in the x-axis is the distance (in meters) and in the y-axis the receiver sensitivity (in dBm). This image shows that in the distance of 139 meters the receiver sensitivity is equal to -70.13 dBm which is less than the theoretically receiver sensitivity in a free space which is -105 dBm.

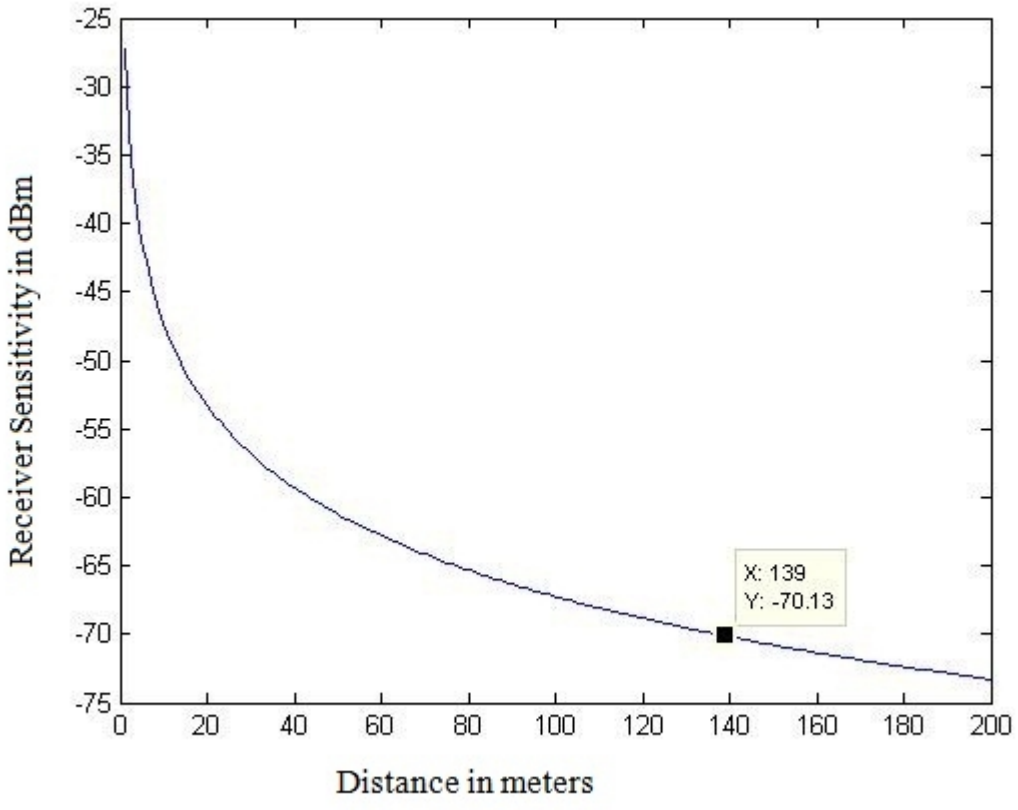

Figure 4.7 Receiver Sensitivity

This difference is due to the environmental conditions that the experiments were happened which weren't ideal. As a result, other factors like humidity, polarization mismatch between antennas, multipath and fading effects due to environment motion and First Fresnel Zone blockage can cause the difference in the receiver sensitivity that was

monitored before. Plane Earth Loss model can better describe the propagation conditions due to the ground reflected ray.

4.2.2 Indoor environment

Coverage issues

In these series of experiments the indoor environment of International Hellenic University was used and more specifically Building A. Image 4.7 illustrates the interior space of that building. The range of reliable communication should decrease due to the number of obstacles that exist in an indoor environment (i.e. walls, doors, desks etc.). The server was put in Lab 1 and was connected to one pc in order to monitor the traffic (the blue spot indicates the position of the sensor) and the other two sensors were put in the following areas:

Table 4: Areas that took place the experiment.

Area	Path Number	Distance from the server in meters	Number of walls
Lecture Room 1	Path 1	31.06	5
Workgroup Room	Path 2	27.02	4
Coffee Shop	Path 3	25.66	3
Conference Hall	Path 4	20.90	2
Stairs	Path 5	14.00	3
WC	Path 6	11.04	3
Lab 2	Path 7	4.53	1
Reception	Path 8	13.85	3

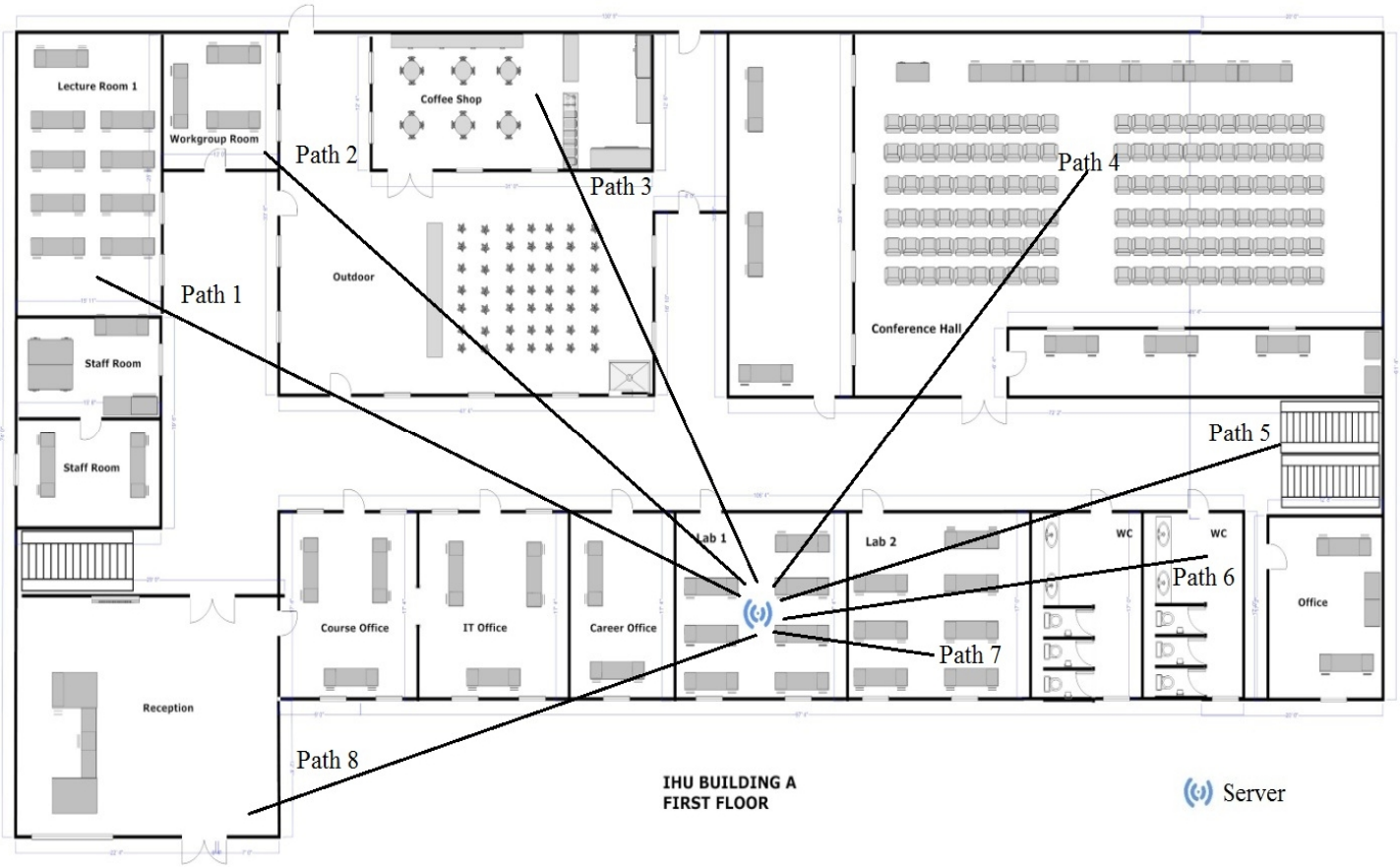

Figure 4.8 Indoor environment of IHU Building A

The results of this experiment showed that in most rooms the server could “hear” simultaneously both sensors, but there were cases like Conference Hall and Workgroup Room where the server could receive packets from only one sensor. In Lecture Room 1 there was no reception or reception of few packets with delay from only one sensor.

Figure 4.8 shows with green the spots where the reception was good, with yellow the spots where the server could receive packets from only one sensor and with red the spots where there was no or very bad reception.

Figure 4.9 Reception map of IHU Building A

As a result, in an indoor environment with many obstacles, the server could receive packets in a distance of 26 meters and above this distance there was no communication. In the Conference Hall the server could receive data from only one sensor although the distance from the server is 20.90 meters. This can be explained due to the fact that this room has thicker walls so the attenuation of the signal is bigger.

In the next phase of this experiment the size of the data packets were increased to 66 bytes. Similarly to the previous experiment, in the outdoor environment the range of reliable data exchange should decrease. The results showed that in Lecture Room 1 there was no reception. Moreover, the reception in Workgroup Room and Conference Hall got worse. The increase in the data length didn't affect the reception in the other areas except the Coffee Shop where sometimes the server couldn't "hear" simultaneously the two sensors.

Image 4.9 shows the "reception map" after the increase in the size of the packets that were transmitting.

Figure 4.10 Reception map of IHU Building A (66 bytes)

Simulation results

In the outdoor environment a small difference between the theoretical receiver sensitivity and the actual receiver sensitivity was monitored. In the next paragraphs an indoor propagation model will be chosen in order to investigate any difference in the receiver sensitivity.

The propagation model that will be used is ITU-R 1238 in which the loss is defined as: [30]

$$Loss = 20 \times \log_{10}(F) + 10 \times n \times \log_{10}(R) + L \times nf - 28$$

Where F is the frequency in MHz, R the distance in kilometers, n the path loss exponent which is equal to 3.2, nf is the number of walls between the transmitter and the receiver and L is the losses that a wall can cause which are equal to10 dB.

Path seven is the path with the minimum number of walls as table 4 shows. The propagation model that was described in the previous paragraph for an indoor environment defines that the maximum distance where the reception is good for a path with only one wall between the receiver and the transmitter is 135 meters. As a result path 7 has good reception in any case.

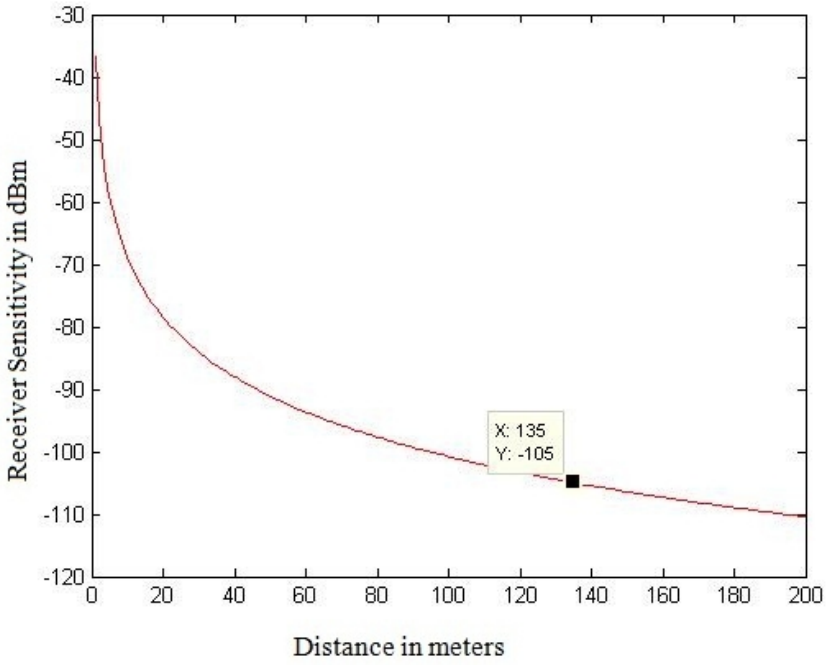

Figure 4.11 Propagation model for path 7

Path 4 is the only one with two walls between the receiver and the transmitter. In this case the maximum distance with good reception is 65.92 meters. The Conference wall where the transmitter was put has thicker walls and this is the reason why the results of the propagation model are different with the results of the experiments.

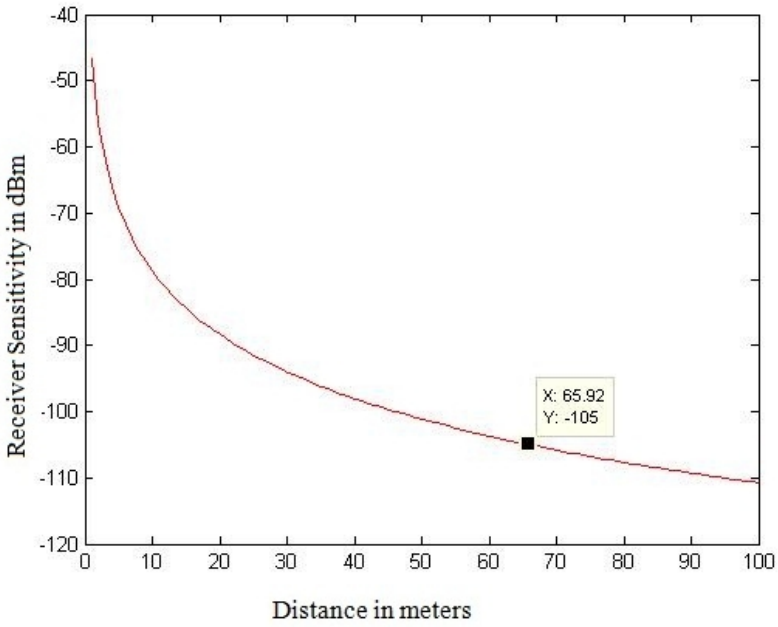

Figure 4.12 Propagation model for path 4

The majority of the paths have three walls in the route between the transmitter and the receiver. The maximum distance for this scenario is 32.09 meters. This is the reason why paths 3, 5, 6 and 8 have good reception in most cases.

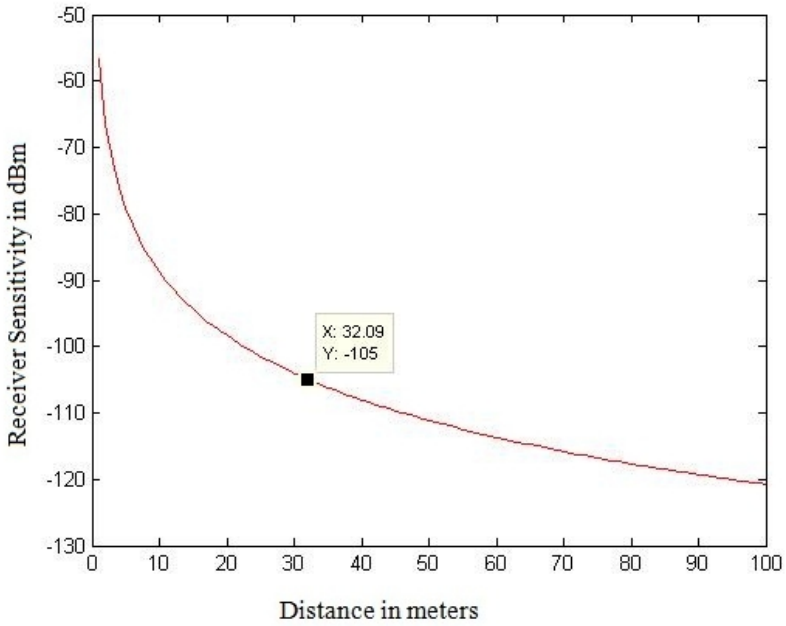

Figure 4.13 Propagation model for paths 3, 5, 6 and 8

The path to the Workgroup room has 4 walls which as it was described in the previous paragraphs didn't have good reception in most of the experiments. The propagation model confirms this finding because theoretically for a path which has 4 walls between the receiver and the transmitter the maximum range of reliable data exchange, as it shown in figure 4.14, is 15.62 meters.

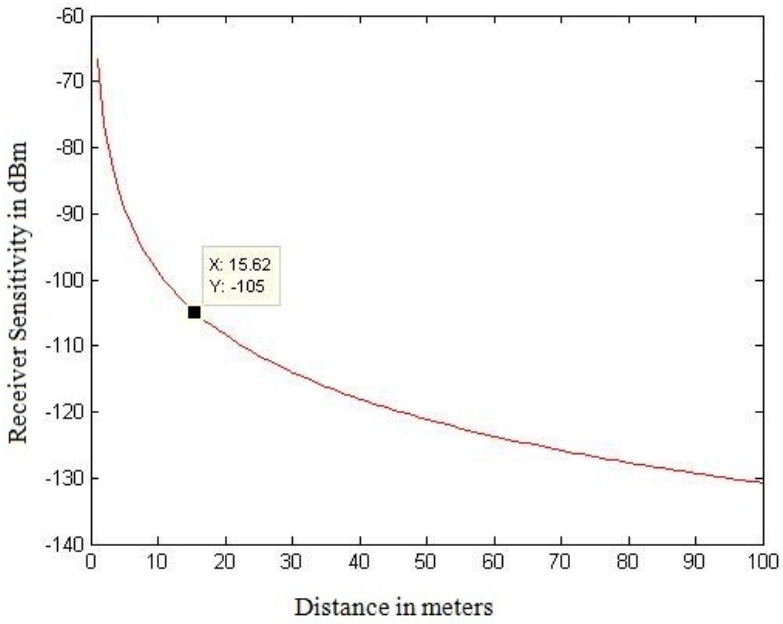

Figure 4.14 Propagation model for path 2

Finally, for path 1 which has five walls between the receiver and the transmitter, the propagation model defines that the maximum range of correct reception is 7.636 meters. As a result it is impossible for Lecture room 1 to have direct communication with the server.

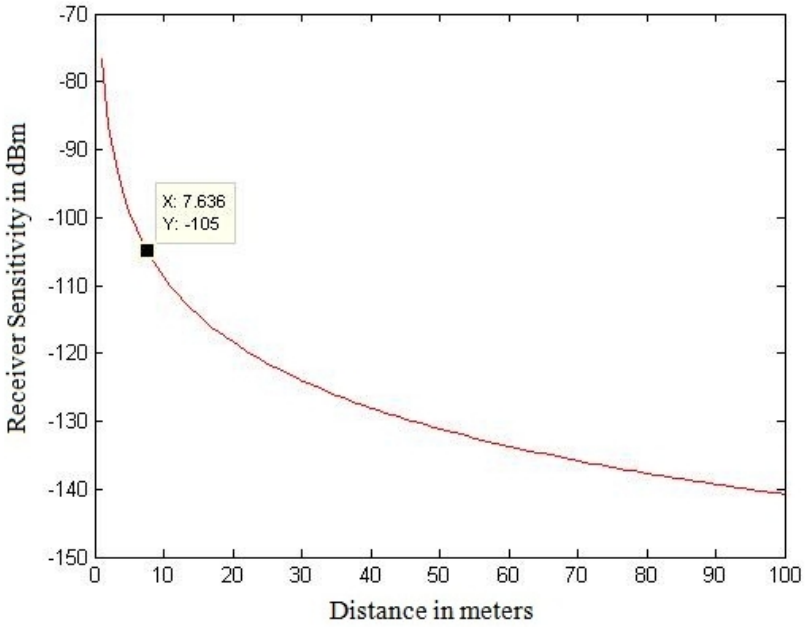

Figure 4.15 Propagation model for path 1

Table 5 is a comparison analysis between the findings of the experiments and the results of the propagation model that was used.

Table 5: Comparison Analysis.

Area	Path Number	Distance from the server in meters	Number of walls	Reception during the experiments	Reception according to the simulation
Lecture Room 1	Path 1	31.06	5	bad	bad
Workgroup Room	Path 2	27.02	4	bad	bad
Coffee Shop	Path 3	25.66	3	good	good
Conference Hall	Path 4	20.90	2	bad*	good
Stairs	Path 5	14.00	3	good	good
WC	Path 6	11.04	3	good	good
Lab 2	Path 7	4.53	1	good	good
Reception	Path 8	13.85	3	good	good

*due to the fact that the walls in this room is thicker

Interference

Interference is an effect that can cause packet losses or packet distortion in a network. Co-channel interference is a crosstalk which is caused by nodes which use the same frequency like the nodes in the experiments that will follow. These experiments took place in the Conference Hall of IHU Building A using five sensors as transmitters and one sensor which was the server. Moreover, the data length or the network topology weren't same in every case in order to monitor how the interference varies.

The first experiment uses the star topology and every sensor was broadcasting its packets. The length of every packet was set to 6 bytes. Figure 4.16 illustrates the position of every sensor in this experiment (The server has blue color and the other sensors are in green).

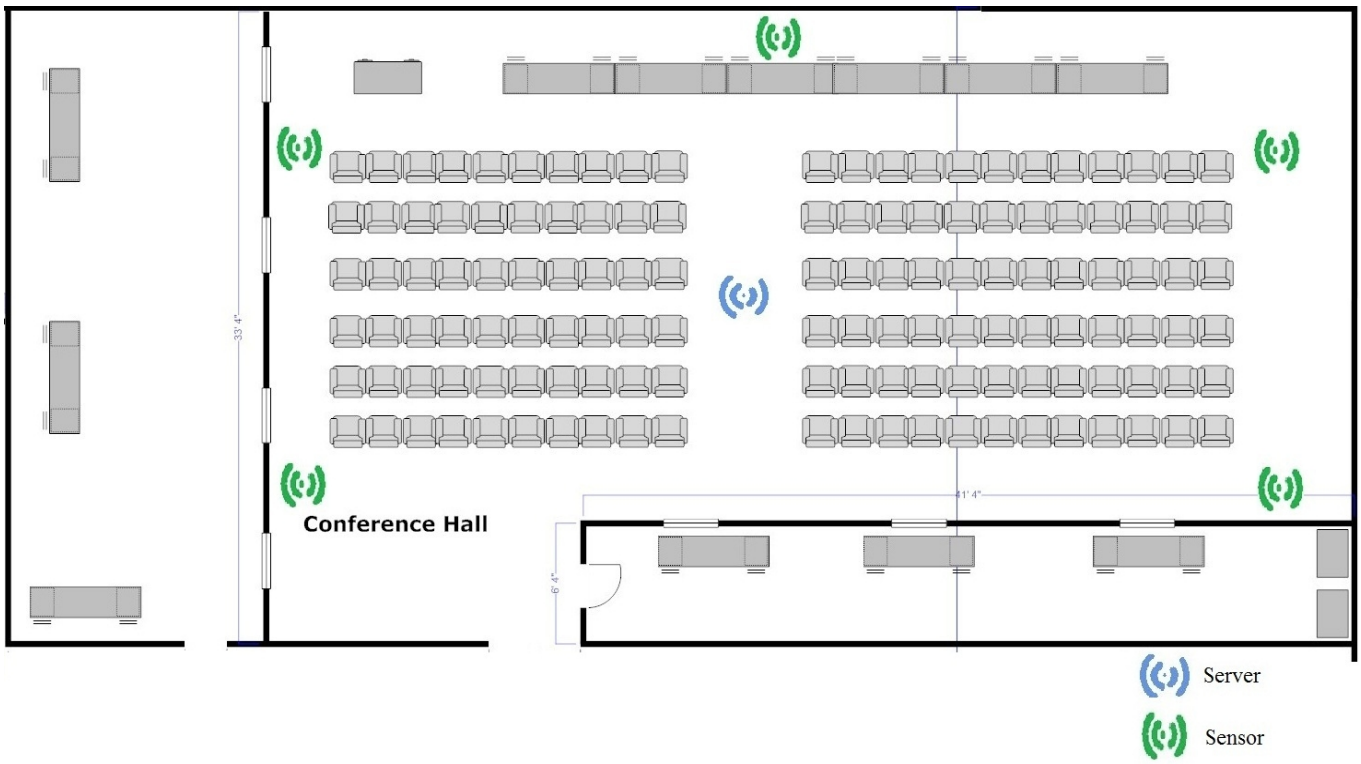

Figure 4.16 Star topology in Conference Hall

Using star topology and broadcasting 6 bytes the server was able to receive all packets from all nodes without any problem at all. In this scenario interference didn't affect the network, making the server able to receive correctly packets from all nodes because the

size over every packet was small. As a result packet losses or packet distortion had very small possibility to happen.

The next scenario of this experiment was to keep the same topology, which is shown to figure 4.16, but with different packet size which increased to maximum and more specifically to 66 bytes. Interference caused 20% to 40% packet losses or packet distortion in this scenario. The server was able to receive packets from three to four sensors and there wasn't any case of receiving packets from all nodes. The packets that were lost weren't from the same nodes but all nodes at certain time couldn't send their data to the destination. In conclusion, using star topology and set the nodes to broadcast packets of 66 bytes increases the affect of interference in the network which results in a significant percentage of packet losses.

Afterwards, the broadcast mode of the sensors changed and all five sensors sent packets of 66 bytes to a specific destination which was the server. The star topology was kept but now the traffic that was generated by five sensors was significant reduced. The server in that case was able to receive packets from all nodes even though they were sending packets with the maximum length. Occasionally the server couldn't receive one packet from the five that it should and this packet wasn't from a specific node. This means that this network can be operational but with setting guarantees about the correct reception of every packet. Moreover, one solution of setting guarantees is the use of acknowledgments for every packet that the server received. As a result every node will know if the server received its data and if not it would send them again.

Until now the network topology that was used was the star topology. In the next series of experiments the topology that will be used is the mesh topology. Five nodes and a server will be connected in a mesh network like in figure 4.17 (With blue color is the server and with green the five sensors).

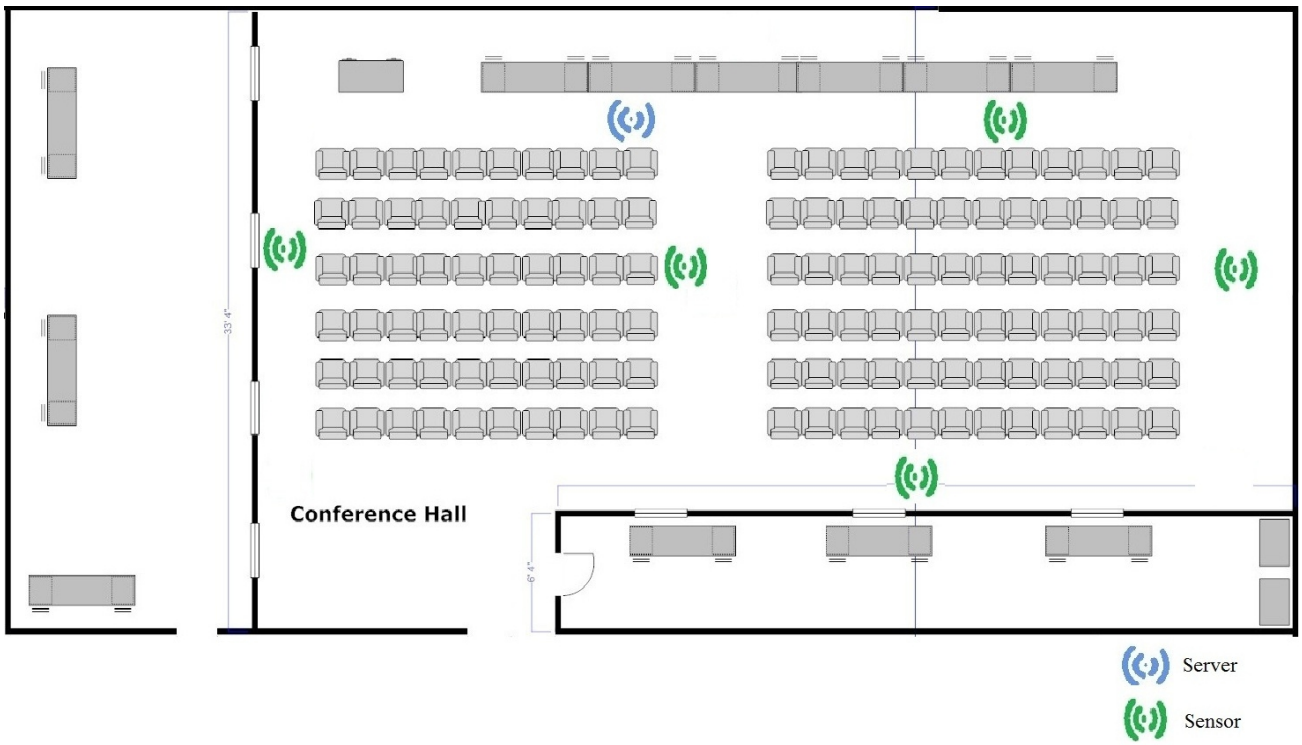

Figure 4.17 Mesh topology in Conference Hall

In the beginning all five nodes were broadcasting packets of 6 bytes and the results showed that like in the star topology the server was able to receive packets from all nodes without any problem. When the size of the packet increased to 66 bytes the server could receive packets from only three sensors which is similar to what happened in star topology. It is worthwhile to mention that the three nodes that were close to the server were monopolizing the network and the other two nodes were let in starvation. This is a significant drawback of the mesh topology where close to the server nodes, when the capacity of the network is very small, can monopolize the entire channel. A solution to this problem can be the increase of the power of transmission to the nodes which are not close to the destination, but this doesn't guarantee that the server will receive packets from all nodes.

The final phase of this experiment uses the same topology but the sensors aren't in broadcast mode but they send their packets to only one destination which is the server. The results of this experiment showed that even if the packet size is increased to 66 bytes, which is the maximum packet length, the network operates without any problem. Occasionally the server couldn't receive packets from the node that appears in the bot-

tom of figure 4.17 but this can be solved with two ways: the increase of the transmission power or the use of acknowledgements.

Table 6: Comparison Analysis.

Mode of data exchange	**Percentage of packet loss**
Star topology with broadcasting 6 bytes	0%
Star topology with broadcasting 66 bytes	20-40%
Star topology unicasting 66 bytes	0-5%
Mesh topology with broadcasting 6 bytes	0%
Mesh topology with broadcasting 66 bytes	20-40%
Mesh topology unicasting 66 bytes	0-10%

5 Mesh Protocol

In this chapter a mesh protocol will be described which can solve the problems that were monitored during the experiments that took place in International Hellenic University.

Furthermore, the biggest goal of this protocol is to establish a reliable communication between the server and the sensors in order to send their measurements. This communication can be direct, if the sensor is in the range of the server, or through another sensor in a case where the transmitter isn't in that range. As a result, with this protocol sensors are not "dumb" anymore but they can take critical decisions.

5.1 Scope of the mesh protocol

The first experiment that took place in an indoor environment (first floor of IHU Building A) showed that there were areas with no or very bad signal which as a result isolates some sensors from the server. In a real mesh network of sensors that is something that should be avoided otherwise the network breaks into pieces.

In the protocol that will be described in detail a sensor doesn't send only its measurements but if it receives data from other sensors it can forward them to the destination. Additionally, when a sensor doesn't have direct communication with the server then it forwards the measurement to one of its neighbors and afterwards it is responsibility of this neighbor the arrival of the measurement to the destination.

Figure 5.1 is the sequence diagram of the mesh protocol that was described in the previous paragraph.

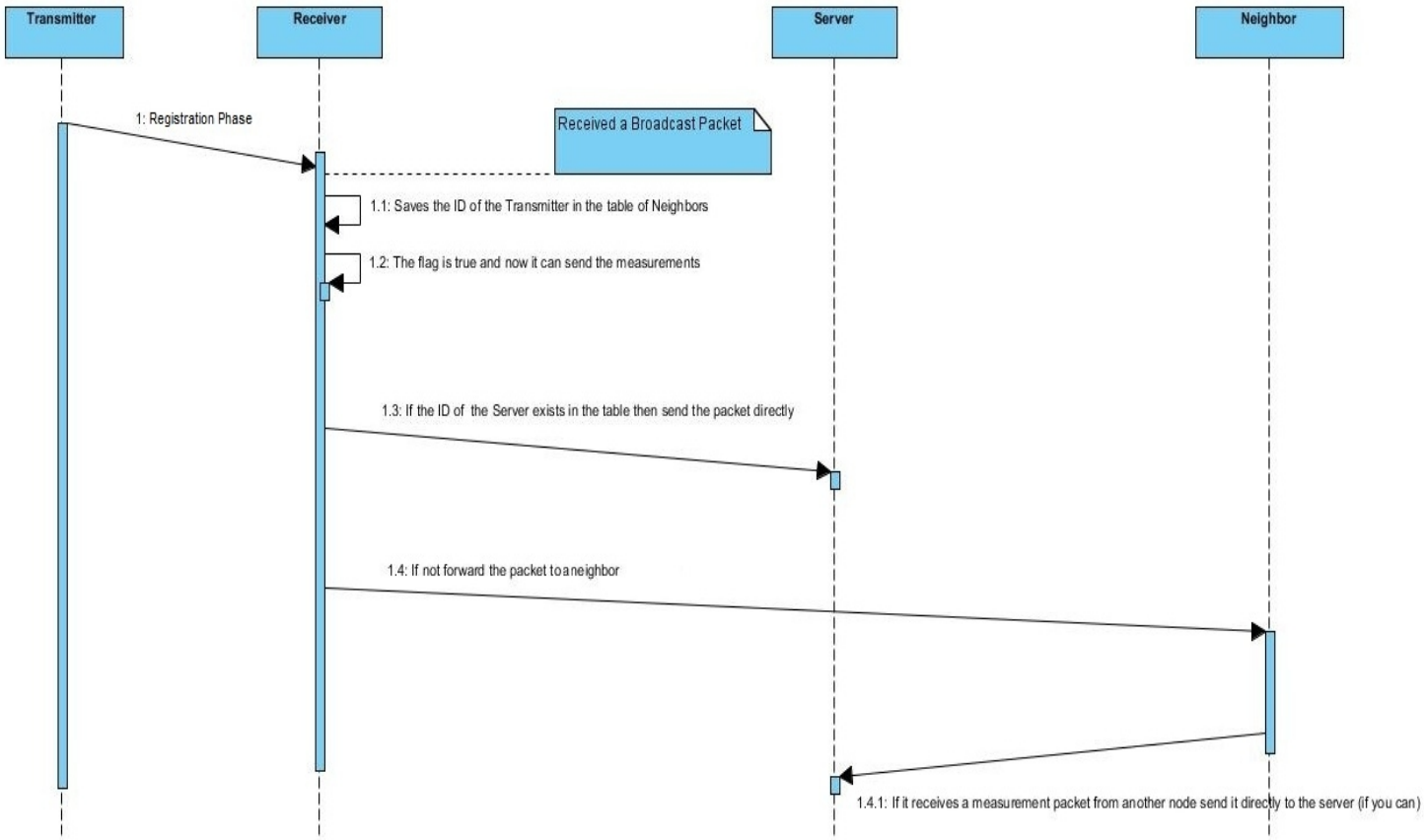

Figure 5.1 Sequence diagram of the Mesh Protocol

5.2 Phases of the mesh protocol

The mesh protocol that has implemented includes three phases:

- Registration Phase
- Data sent phase
- New sensor registration phase

5.2.1 Registration Phase

The initial phase of this protocol is the registration phase where all nodes broadcast a packet. This broadcast packet informs the receiver that the transmitter is a neighbor and as a result it is in its range. If the sender is the server the node knows that it has direct communication with it. In this case this node sends its measurements directly.

If a node receives a broadcast packet from another node, except server, then it saves the ID of the sender in a table which includes the ID's of all neighbors, but before it performs this action it controls if this ID exists in that table in order to avoid an overflow. Another control that it can be done from the receiver is to investigate how many packets it received during the duration of the registration phase. If the percentage of the received packets is above a threshold then it is allowed to save the ID of the sender in the neighbor list (this control isn't included in this protocol yet). Moreover, after this phase every node knows which are its neighbors and it can take decisions about how to send its measurements to the server. Figure 5.2 shows an example of the registration phase.

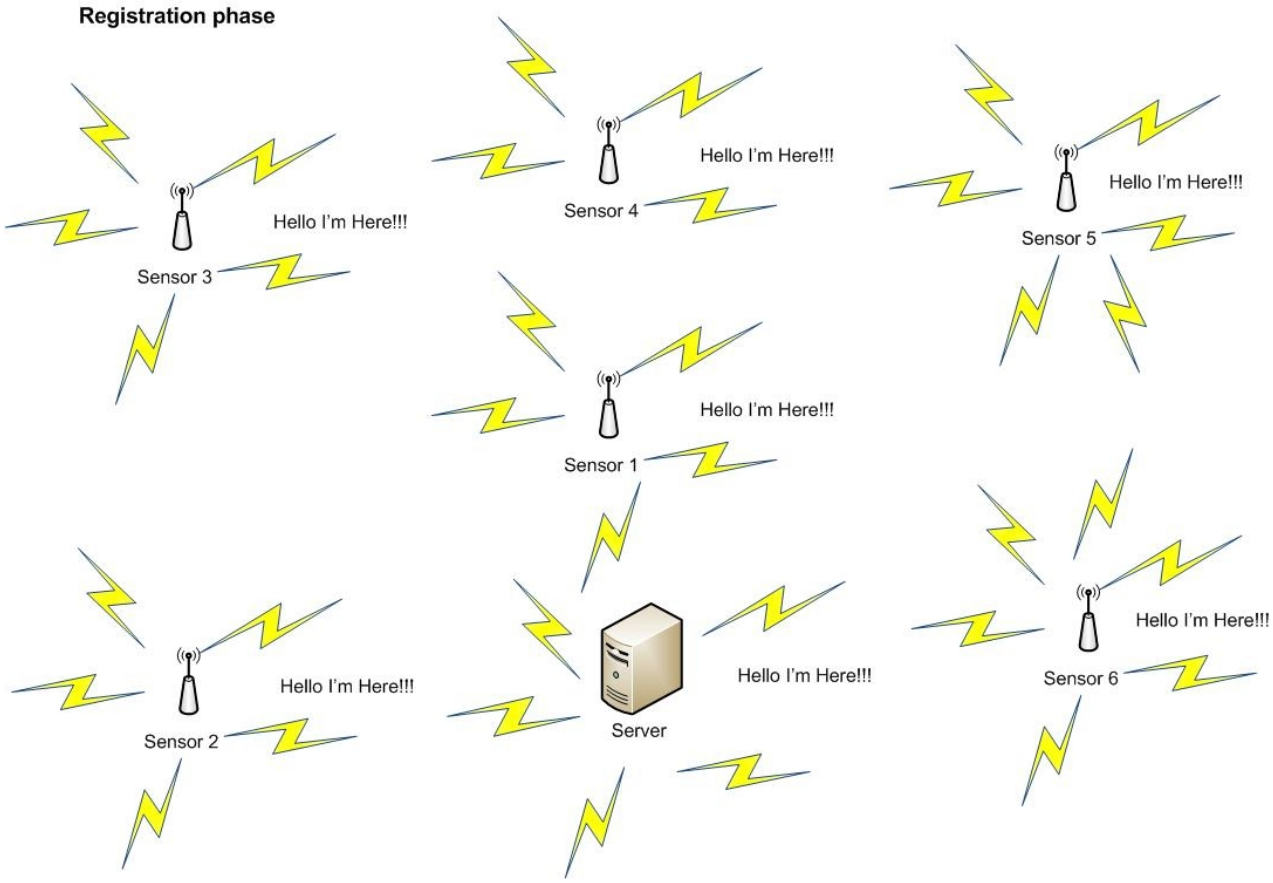

Figure 5.2 Registration phase

The duration of this phase is six seconds and during this time all nodes broadcast a packet every second. When this phase is completed all nodes knows their neighbors like in figure 5.3 where the ID's of the neighbors are saved in a table.

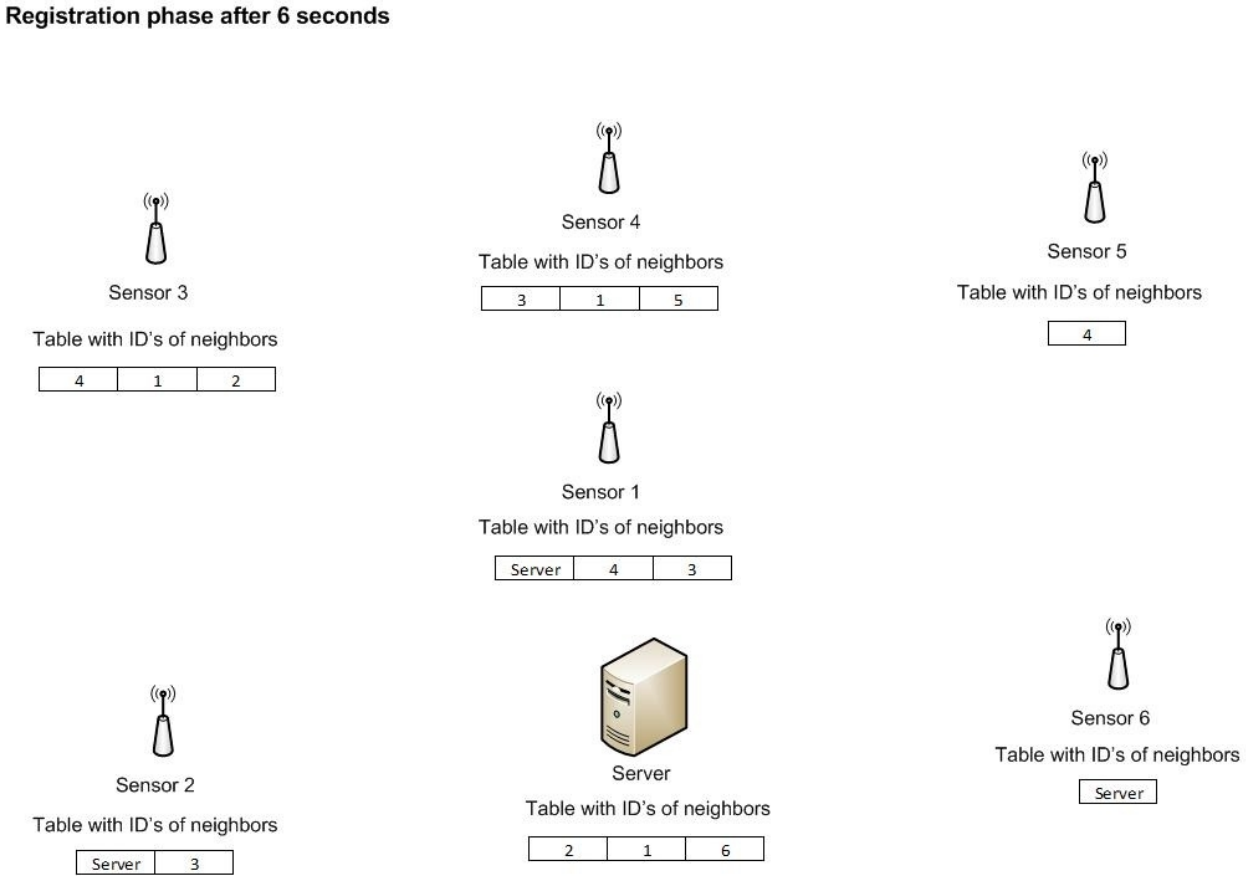

Figure 5.3 Completion of registration phase

5.2.2 Data Sent Phase

The next phase begins when the registration phase is completed. In this phase the nodes want to send its measurements to the server. To do this they have to decide if they will forward the packet or they will send it directly to the server. The table which contains the ID's of the neighbors will help them to take that decision. When a node wants to send its measurement first it scans the table with the ID's to find out if the ID of the server exists, if so it sends it directly or in the opposite case it forwards the packet to a neighbor.

Furthermore, with this protocol the sensors are not dumb anymore but they can take critical decisions. When the ID of the server doesn't exist in the table with the ID's of

the neighbors, then the sensor picks a random cell from the table and it sends its measurement to the sensor with the ID that it picked up before. With this operation a certain node is not loaded over time which may collapse it. For example if a node is a neighbor of the server and it has many neighbors which don't have direct communication with the server, then if all neighbors try to send its data through this node then it is almost certain that it will collapse. In the opposite way if all sensors are trying to explore new routes this can avoid the overload of specific nodes. This is the reason why when a sensor doesn't have direct communication with the server it picks up a random neighbor to forward the packet. This neighbor in the next measurement that the node will transmit it has large probability to differ.

Moreover, when a sensor receives a packet that it is a measurement then it knows that it has to send it to the server, if it is neighbor of the server, or it should forward to another neighbor.

In contrast, zigbee or IEEE 802.11s which use AODV routing have a different perspective. With AODV the channel is used not only for transmitting measurements but also for broadcasting route requests (RREQ) and route replies (RREP). In addition, sending and receiving RREQs and RREPs demands more RAM use from the sensors. All these differ from the designing goals of the mesh protocol that has been implemented.

The time that is needed for every hop it is measured and the results showed that it varies from one to three milliseconds. This variation is due to the fact that every sensor before it sends a measurement first it hears the channel in order to detect a carrier. If the channel is free then it transmits immediately the packet. In other case the transmission will be delayed.

Image 5.4 is an example of this phase where sensor 3 which doesn't have in its table the ID of the server, sends the packet to sensor 2. Afterwards, sensor 2 sends the measurement to the server. On the other hand, sensor 6 sends directly its packet to the server because it is neighbor of the server.

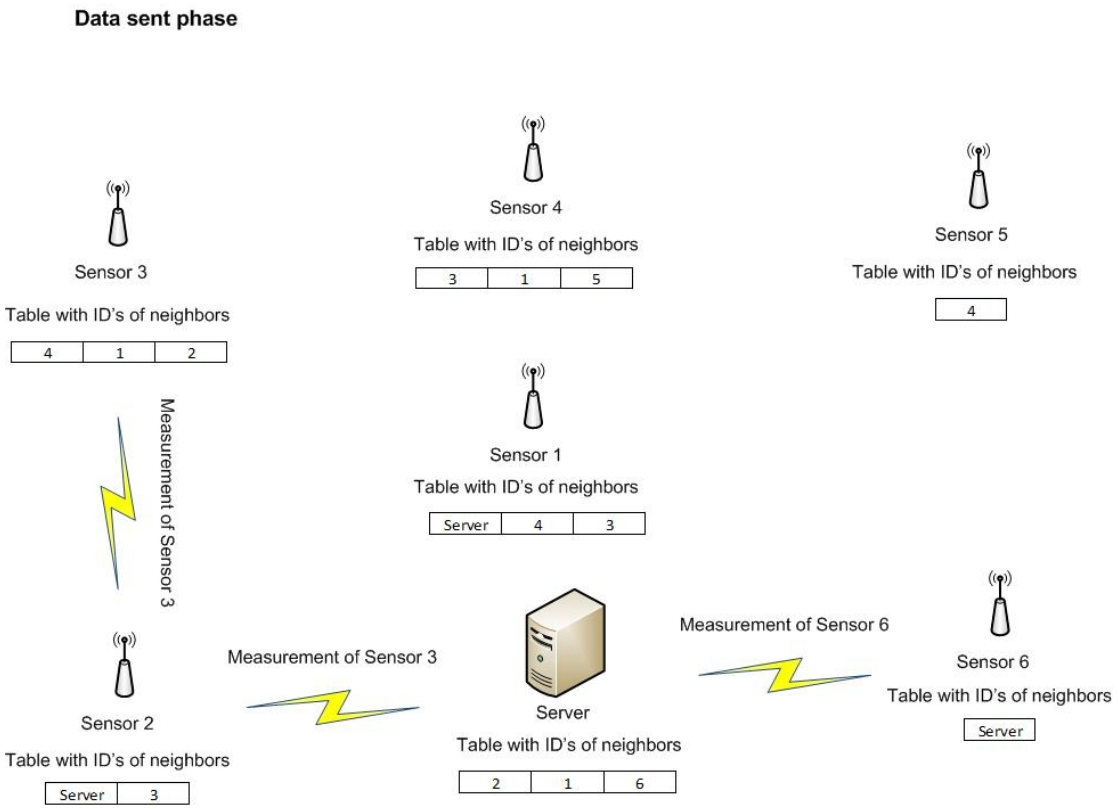

Figure 5.4 Data sent phase

5.2.3 New sensor registration phase

This mesh protocol can be used in networks where the size of them isn't static but it can increase with the addition of new nodes. Furthermore, after the registration phase all sensors can "hear" the channel for broadcast packets. If that happens then the node that receives it saves the ID of the transmitter in the table with the neighbors but also replies to the sender with an ACK, in order to know that it is in its range.

For example, in the network that is shown in figure 5.5 sensor 7 is a new addition to the network which immediately sends a broadcast packet. Sensor 5 and sensor 6 receive the packet and they correspond with an ACK. Moreover, the neighbor list of sensor 5 and sensor 6 now include one more cell with the ID "7".

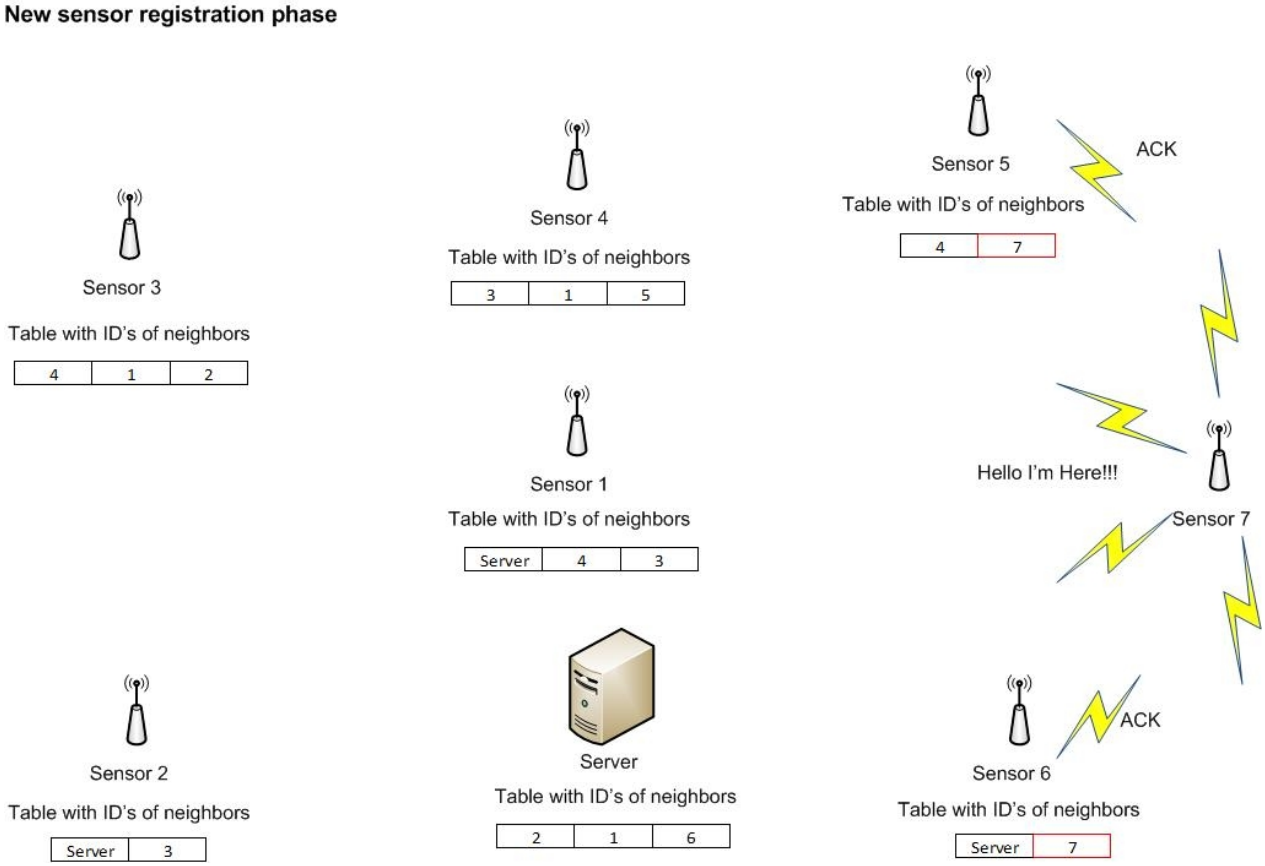

Figure 5.5 New sensor registration phase

5.3 RF 12 packet format

The mesh protocol that was implemented and described in the previous paragraphs supports only RF 12 packets. The format of a RF 12 packet is shown in the next figure:

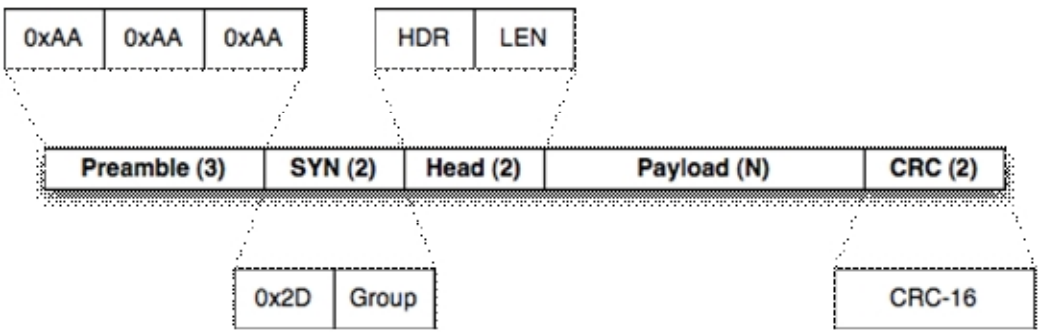

Figure 5.6 RF 12 packet

The payload of a RF 12 packet which carries the data of every packet has 66 bytes length in order to keep the use of RAM in low levels. Moreover, the total length of a RF 12 packet as it can be noticed is very small because longer packets demands more time to process which as a result increases the energy consumption.

The network group is one byte and also doubles as second SYN byte. The node ID is five bits in order to allow few more header bits in the same byte.

5.3.1 Header of RF 12 packet

There are only three header bits which are:

- The A bit (ACK) indicates whether this packet wants to get an ACK back. In that case the C bit must be zero.
- The D bit (DST) indicates whether the node ID specifies the destination node or the source node. For packets sent to a specific node, DST is equal to one. For broadcasts, DST is equal to zero, in which case the node ID refers to the originating node.
- The C bit (CTL) is used to send ACKs, and in turn must be combined with the A bit set to zero.

As a result there is only one room for either the ID of the source node or the ID of the destination node. To summarize the previous, the combinations that we can have are the following:

- Normal packet with no ACK requested: CTL = 0, ACK = 0.
- Normal packet with ACK requested: CTL = 0, ACK = 1.
- ACK reply: CTL = 1, ACK = 0.

The header of a RF 12 packet can be seen in figure 5.7.

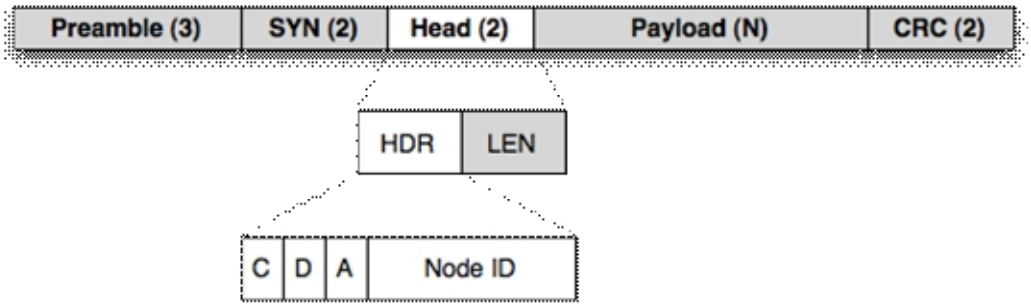

Figure 5.7 Header of RF 12 packet

5.3.2 Payload of RF 12 packet

The mesh protocol has designed in such a way that when a packet arrives in the destination the receiver knows the number of hops and the ID of every hop. The header of a RF 12 packet can contain the source ID or the destination ID which is a limitation for the mesh protocol. As a result, the payload of the RF 12 packet doesn't contain only the measurement but also the source of the measurement and the ID's of the hops.

Furthermore, the first 20 bits contain the measurement which can carry data for the temperature, the level of lighting and the humidity. An example of this 20 bits can be the following: "M:+24°C,40%,400lx" where the letter "M" indicates that this packet is a measurement and not a broadcast packet, the temperature is +24 degrees of Celsius, the humidity 40% and the lighting 400 lux.

The 21th bit contains the ID of the sensor that made this measurement and all the rest is used for the routing that this packet followed. An example of the payload of the RF 12 packet is shown in figure 5.8.

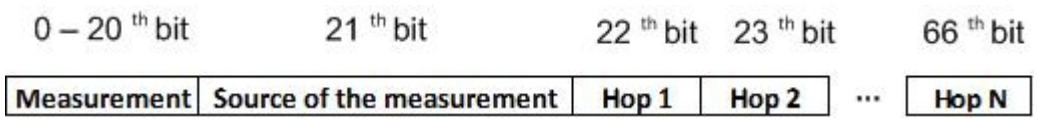

Figure 5.8 Payload of RF 12 packet

5.4 Carrier detection

Wireless communication is a very complex process. Rules must be taken in order to avoid transmissions interfering, which means that only one transmitter can be active at a specific time in the same frequency band. This is called CSMA/CA where all nodes are trying to find a free slot to transmit their data.

The RF 12 driver includes the method “rf12_can_send” in order to sense the channel for a carrier. The RF12 driver code looks at the RSSI status bit before starting to transmit. If a carrier is detected, even one that isn’t being recognized by the RFM12B, then transmission will be delayed. The code for the rf12_can_send is the follow:

```
uint8_t rf12_canSend () {
    // no need to test with interrupts disabled: state TXRECV is only reached
    // outside of ISR and we don't care if rxfill jumps from 0 to 1 here
    if (rxstate == TXRECV && rxfill == 0) {
        cli(); // start critical section so we can call rf12_xfer() safely
        if (rf12_xfer(0x0000) & RF_RSSI_BIT) {
            // carrier sensed: we're over the RSSI threshold, don't start TX!
            sei(); // end critical section
            return 0;
        }
        rf12_xfer(RF_IDLE_MODE); // stop receiver
        //XXX just in case, don't know whether these RF21 reads are needed!
        rf12_xfer(0x0000); // status register
        rf12_xfer(0xB000); // fifo read
        rxstate = TXIDLE;
        sei(); // end critical section
        return 1;
    }
    return 0;
}
```

5.5 Simulation results

Until now the experiments showed the rooms that didn’t have good reception and if that was a real network it is sure Lecture Room 1 and maybe the Conference Hall wouldn’t be able to send their measurements to the server.

The sensors that were used in these series of experiments remained in the same places but they used the mesh protocol that was described previously. One sensor was put in Lab 1, which was the server, and the rest were put in Lecture Room 1, Conference Hall, Reception, Coffee Shop and Stairs. The two sensors that were in Lecture Room 1 and

Conference Hall didn't send their packet directly to the server but through other sensors (Reception and Stairs respectively). Image 5.9 shows the map of this network.

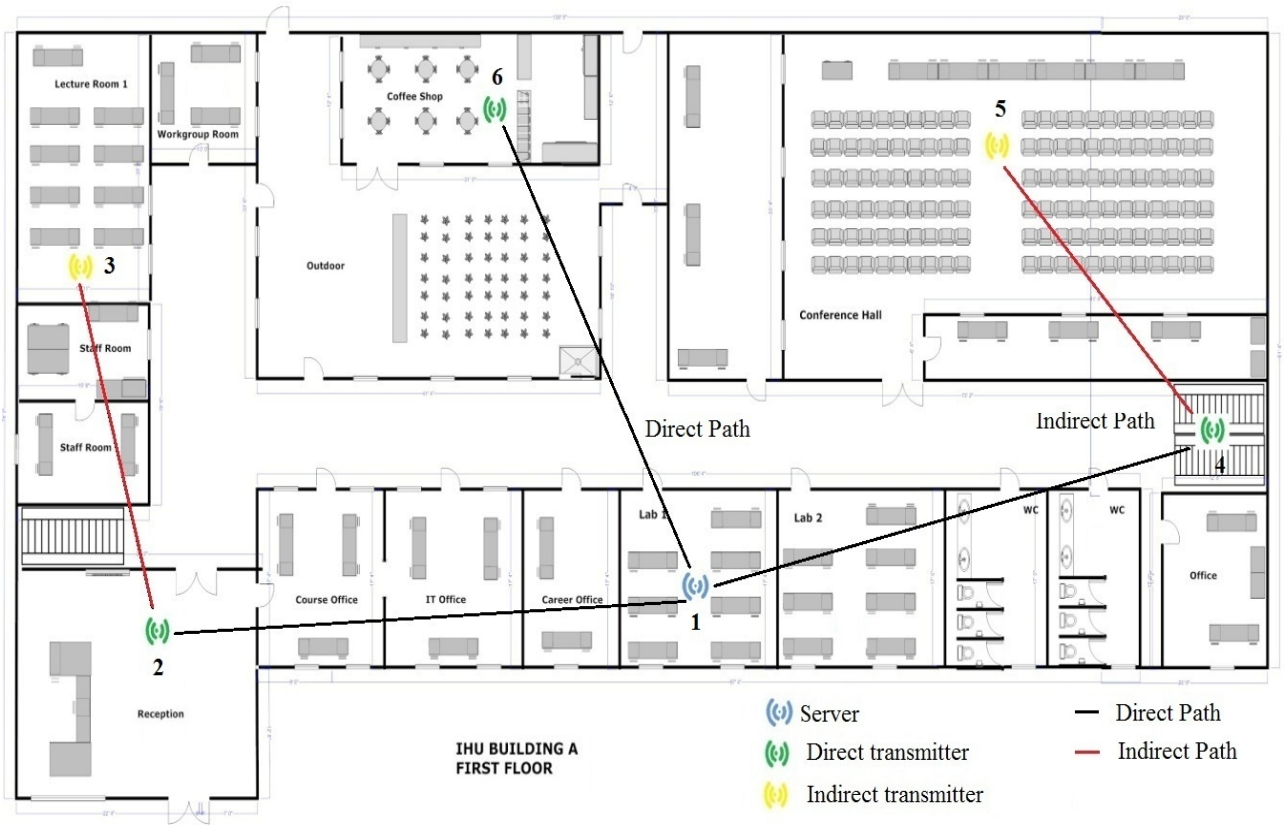

Figure 5.9 Reception map of the mesh network

As a result the server was able to receive data packets from all nodes without any problem. Even though there were sensors in the previous experiments that couldn't send their data to the server, with this solution every sensor was able to send its data to the server directly or through another sensor. Figure 5.10 shows the serial monitor of the server.

In this network if more sensors were added, then as a result more paths can be created. Additionally, figure 5.9 shows that the sensors which don't have direct communication with the server choose only one specific node to forward its data, but with the addition of more sensors then every sensor can choose a random neighbor from its neighboring list.

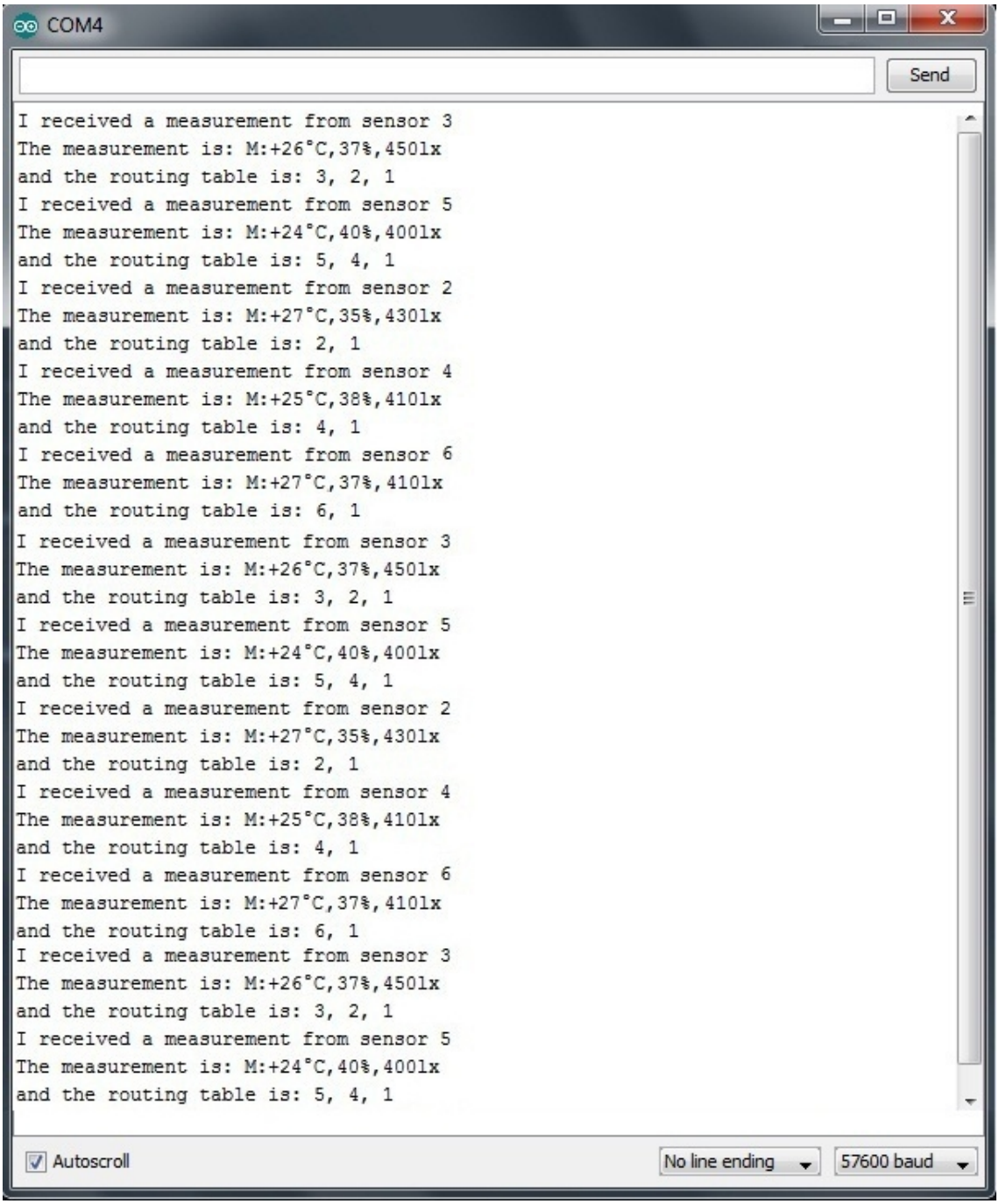

Figure 5.10 Serial monitor of the server

As figure 5.10 shows, sensors with ID's 3 and 5 send their packets through sensors with ID's 2 and 4 respectively. In contrast, sensors with ID's 2 and 4 send their data directly to the server. Moreover, the server is able to know the path that every measurement has followed.

Afterwards the length of the packet size was increased to 66 bytes. The server was receiving again packets from all sensors without any serious problem. In that case the traf-

fic was distributed because all nodes didn't send their data simultaneously which can cause delays or packet losses, but the existence of two sensors that were acting like repeaters had as a result the segmentation of the traffic.

The implementation of the mesh protocol has the following advantages:

- Every sensor has a reliable communication with the server directly or through another sensor.
- Interference is minimized and it doesn't cause packet losses or packet distortions.
- The server is able to know the path that every measurement has followed.
- The traffic of the network is segmented.
- All sensors pick a random neighbor to forward their data which as a result doesn't lead to an overload of a certain node.
- If a new sensor is added to the network all sensors that are in its range are informed.
- The mesh protocol can be functional even if the packet size is increased to the maximum length (66 bytes).
- Decrease of energy consumption because there is no need to increase the power of transmission of nodes that aren't in the range of the server.

6 Conclusions

The goal of this dissertation was to investigate practical aspects of a wireless mesh network. Different network topologies and standards for advance metering infrastructure were theoretically described in chapter two and three.

Afterwards, several sensors were connected using different topologies in order to explore coverage issues, interference and other characteristics of these networks. In chapter four the experiments showed that the maximum coverage in an outdoor environment is 139 meters with a normal packet size (6 bytes). This range reduces if a new sensor is added to the network or if the packet size is increased.

Furthermore, the experiments that took place in the indoor environment of the International Hellenic University showed that in average the maximum range that a transmitter and a receiver can have reliable communication is approximately 26 meters. This number depends on the number of walls or generally the number of obstacles that exist between the transmitter and the receiver. The propagation model that was used and described in detail, confirmed the findings of these experiments.

Moreover, the experiments in the indoor environment of International Hellenic University showed that all rooms couldn't have direct communication with the server. As a result a mesh protocol was implemented in order to solve this problem. With this protocol when a node doesn't have direct communication with the server, it sends its data to a random neighbor who is responsible to forward it to the server. This mesh protocol was tested and the results showed that every room in International Hellenic University had a reliable communication with the server without any problem. Even if the packet size is increased to maximum (66 bytes), the protocol guarantees that the network will be stable.

As it said before, the mesh protocol that was implemented chooses a random neighbor in order to forward the data when a direct path doesn't exist. Our future work is to redesign the protocol and to use a routing algorithm like a link state or a distance vector routing algorithm. This protocol proved that it operates fine in any case that was tested but in our future plans is to follow a different perspective which is to enrich it with a standard routing algorithm.

Bibliography

[1] P. Santi, “Topology control in Wireless Ad Hoc and Sensor Networks”, John Wiley & Sons, Ltd.

[2] Eiman Alotaibi, Biswanath Mukherjee, “A survey on routing algorithms for wireless Ad-Hoc and mesh networks”, Elsevier

[3] Yu-Chee Tseng, Shih-Lin Wu, “Wireless Ad Hoc Networking”, Auerbach Publications.

[4] Xudong Wang, Weilin Wang, Ian F. Akyildiz, “Wireless mesh networks: a survey”, *Elsevier,* June 2004.

[5] Toby Skandier, David Groth, “Network”, Wiley Publishing Inc..

[6] Larry Friedman, “SimpliciTI: Simple Modular RF Network Specification”, Texas Instruments, Inc.

[7] “TI-MAC - IEEE802.15.4 Medium Access Control (MAC) Software Stack”, Texas Instruments, Inc.

[8] “RemoTI Developer's Guide”, Document Number: SWRU198, Texas Instruments, Inc.

[9] Raffaele Bruno, Conti, M., Gregori, E., “Mesh Networks: Commodity Multihop Ad Hoc Networks”, *IEEE Communications Magazine,* March 2005.

[10] L. Klein-Berndt, “A Quick Guide to AODV Routing”, *.National Institute of Standards and Technology.*

[11] Richard G. Ogier, Bhargav Bellur, “A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks”, *INFOCOM '99,* March 1999.

[12] Richard G. Ogier, "Proposed Changes for TBRPF", *SRI International*, August 2001

[13] B. Central Power Research Institute, "Smart grid technology – Business opportunities", June 2010.

[14] Forrest Small, Tom Brunetto, Frances Cleveland, "Smart Grid: Interoperability and Standards An Introductory Review", *Utility Standards Board,* September 2008.

[15] Malay Thaker, Roland Acra, "Internet Standards Come to the Advanced Metering Infrastructure", *Electric Energy Publications Inc.*.

[16] D. DeBlasio, "Status of Standards for the Smart Grid", *IEEE Standard Board Meeting,* 28 January 2009.

[17] C. Lima, "Smart Grids IEEE P2030", *ETSI Workshop - Standards: An Architecture for the Smart Grid,* 5 April 2011.

[18] Jinyun Zhang, "The Latest Development of Smart Grid Standards and Pilot Projects", Mitsubishi Electric Research Laboratories, Inc., November 2010

[19] T. Basso, "IEEE P2030 Development General Concepts", *IEEE P2030 Smart Grid Interoperability Standards Development Kick-Off Meeting,* 3 June 2009.

[20] Richard DeBlasio, Thomas Basso, "IEEE Smart Grid Series of Standards IEEE 2030", *Grid-Interop 2011,* 5 December 2011.

[21] K. Schwarz, "Telecontrol Standard IEC 60870-6 TASE.2 globally adopted".

[22] E. Knapp, "Securing Critical Infrastructure Networks for Smart Grid", Elsevier.

[23] Stefano Galli, Anna Scaglione, Zhifang Wang, "For the Grid and Through the Grid: The Role of Power Line Communications", June 2011.

[24] N. Theethayi, J. Anatory, "Broadband Power-line Communication Systems", WITPRESS.

[25] Hendrik C. Ferreira, Lutz Lampe, John Newbury, Theo G. Swart, "Power Line Communications: Theory and Applications for Narrowband and Broadband Communications Over Power Lines", John Wiley & Sons.

[26] P. Grossetete, "IEEE 802.15.4g Smart Utility Networks (SUN) Overview", *Cisco*

Developer Network.

[27] M. T. Garrison Stuber, A. F. Snyder, "The ANSI C12 protocol suite - updated and now with network capabilities", *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2007. PSC 2007,* March 2007.

[28] Stefan Feuerhahn, Zillgith, M., Wittwer, C., Wietfeld, C., "Comparison of the Communication Protocols DLMS/COSEM, SML and IEC 61850 for Smart Metering Applications", *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference,* October 2011.

[29] Association, DLMS User, COSEM Architecture and Protocols.

[30] Simon R. Saunders, Alejandro Arago´ N-Zavala, "Antennas and Propagation for wireless commuications systems", John Wiley & Sons, Ltd.

Appendix

```
/*
  Method that is used in order to initialize the nodes. As we can see
  in the function "rf12_initialize" the first argument is the ID of the
  node, the second is the band and the third the group that this node
  belongs. Furthermore, the Serial monitor is set to 57.600 baud.
*/

void setup () {
    Serial.begin(57600);
    rf12_initialize(NodeID, RF12_868MHZ, 212);
}
```

Set Up Method

```
If it passed 6000 milliseconds then the sensor sends its measurement.
*/

if (sendTimer.poll(6000)){

  flag = false;         // This will stop the registration phase to trigger again

  randNumber = random(0, sizeof(IDofNeighbors));    // Choose a random Sensor of the neighbors


  measurement[21] = (char)NodeID;       // The 21th cell of the packet includes the ID of the sensor that created this packet

      if(Contains(DestinationID)){           // Check if the sensor has direct communication with the server. If it has the sensor sends directly the packet.

            if (rf12_canSend()){

            rf12_sendStart(RF12_HDR_DST | DestinationID, measurement, sizeof measurement);

            }

      }

      else{                 // If the sensor doesn't has direct communication with the server it forwards the measurement to a random neighbor.

            if (rf12_canSend()){

            rf12_sendStart(RF12_HDR_DST | IDofNeighbors[randNumber], measurement, sizeof measurement);

            }

      }

}
```

Method for sending the measurements

```
/*
The following if-clause checks if the sensor that the packet will be forwarded is the same
with the sender.
*/
if(IDofNeighbors[randNumber] != buf[2l] && IDofNeighbors[randNumber] != buf[temp]){



rfl2_sendStart(RFl2_HDR_DST | IDofNeighbors[randNumber], buf, sizeof buf);


}

else{

  if(randNumber + l < sizeof(IDofNeighbors)){

    rfl2_sendStart(RFl2_HDR_DST | IDofNeighbors[randNumber + l], buf, sizeof buf);

  }

  else{

    rfl2_sendStart(RFl2_HDR_DST | IDofNeighbors[randNumber - l], buf, sizeof buf);

  }


}
```

If - clause which sends the measurement to a random neighbor