

Modelling and analyzing different MAC layers over PLC

Guillermo J. Ravera Iglesias

Enginyeria i Arquitectura La Salle

University Ramon Llull (URL)

Barcelona, Spain

{gjravera}@salleurl.edu

Abstract— Nowadays PLC networks have achieved quite importance in control networks. PLC network allows making an efficient deployment of the control network, taking advantage of the existing power networks. This paper is focused on analyzing different medium-access protocols, which are modelled with OPNET 11.5. Furthermore, the objective of the implemented models is obtaining comparative results of the different simulated MAC layers.

Index Terms—AMR, PLC, Metering, PLC MAC NB.

I. INTRODUCTION

THE development of new devices which are able to communicate through PLC networks has changed its goal. Nowadays, these networks are not only for power distribution; they add new applications such as AMR (Automatic Meter Reading).

AMR is the action of reading a meter without the needing of accessing physically to it. The reading can be done either over PLC networks or any others, for example RF (Radio Frequency) networks. The remote meter reading improves customer services by giving accurate billing, fraud detection and others services.

AMR is implemented in the application layer over the MAC layer, this layer is the most important because it defines the functionality and restrictions of the upper layers. There are several specifications regarding to the application layer i.e.: IEC-61334 or CEA709-1B. Nevertheless they are focused on communication mechanism and not in the management of the power network devices. Actually, Management mechanisms are responsible of addressing schemes, synchronization, logical topology and more tasks that allow end-to-end communication. The main problem we have already found, and is not provided by the previous specifications, is that we

need both features: communication and management mechanisms. For this reason we use “*Remote reading Project MAC PLC-NB Level*” on the basis of the implemented models, because this protocol provides management and communication mechanisms.

This paper is divided in three parts.

Within the first part, the characteristics of the analogical medium (power bus), its implementation with OPNET and the changes to be done to the OPNET bus pipeline stages are explained. These changes must be done to achieve the analogical behaviour of the power bus.

Within the second part, details about the performance of the implemented protocols in OPNET are given. This part also explains the aspects of each implementation that will be analyzed latter in this paper.

Through the third and last part of this paper, the results of each simulation are shown: the time needed to associate all the devices in the physical network on a tree logical network, the overhead needed by the MAC layer to synchronize the overall network, the time required to interrogate all the devices in the network and finally the distribution of the devices in the logical network generated.

II. PLC MEDIUM

A. PLC medium characteristics

The PLC medium can be modelled as an analogical medium where the attenuation, coupling and interference through the power line will be modelled. The coupling between the power lines is provoked because of the physical topology of the power networks. There is a central device which distributes the power to all remote meters. The wires connected to the central device are more prone to couplings than the wires that are interconnected to a group of remote meters.

B. Modelling PLC medium in OPNET.

The bus implementation done with OPNET is a typical digital bus, where collisions and BER are a consequence of the lost packets. Some analogical effects such as attenuation, interference between pairs or reception zones are not taken into account. These analogical effects should be simulated and consequently added in the OPNET implementation.

In OPNET there are a group of phases used to model the transmission of a packet through the PLC network. These phases are called pipeline and are used to model the characteristics of the transmission medium. The names of the phases are transmission delay, closure, propagation delay, collision, error allocation and error correction. The transmission delay phase calculates the amount of time needed to put the whole size of the packet in the medium. The closure phase calculates whether each receiver will be able to receive the packet. The propagation delay phase computes the amount of time needed by the packet to arrive at its destination. The collision phase computes the number of collisions suffered by an individual transmitted packet. The error allocation phase computes the bit error tax within the packet based on the BER extracted from the bus. The error corrections are done through the last phase and determine if the receiver can process the packet. This decision is based on the number of errors tolerated by the receiver and the number of errors suffered by the packet through its transmission.

These 6 phases are used to model all the characteristics of a digital bus, and just modifying them, we can model any behaviour needed. The changes introduced in these phases to reflect the characteristics of a PLC medium will be described later on in this paper.

The closure phase of the pipeline has been modified to reflect the attenuation across the bus. The packet contains a field called attenuation which reflects the attenuation of the packet in several retransmissions along the bus.

The error allocation phase has been modified to calculate the error allocation in two parts. The first part is the header and the second part is the body. This is a transmission requirement of the protocol "*Remote reading Project MAC PLC-NB Level*".

The error correction phase has been modified to monitor the collisions through the medium at the MAC layer. The original behaviour is discarding these packets at this stage. Another change carried out in this phase was the capability of checking the BER in two different parts: header and body (if this last exists).

There is one of the characteristics of the PLC medium that cannot be modelled with the pipeline; it is the coupling between wires. The HUB is a new model implemented in OPNET, which function is interconnecting 3 wires in order to be able to model transparent retransmissions and reception zones. With this new model all the characteristics of a PLC medium have been modelled in OPNET.

The modelling of the HUB has not been simple because of

the transparent transmission requisite. In OPNET any transmission and reception have a delay implicit to the transmission delay explained in the pipeline, the transmission phase. This provokes an undesirable delay in the retransmissions of the HUB model. This delay does not meet the goal of the model and because of this, a forced transmission has been implemented. This implementation consist to save a copy of the packet to transmit on the hub prior to transmission, when the transmission initiate and the HUB detects the channel busy, it immediately transmit the saved packet without waiting to receive the entire packet and avoiding the delay introduced by the transmission phase. With this implementation the transparent transmission is achieved.

III. MAC LAYER PROTOCOLS

Two MAC layers were implemented and analyzed. The layers behaviour is explained next.

The first MAC layer is named "MAC PLC-NB Level". This implementation divides the communication in two periods (interrogation and contention). Each of these periods has its own communication method. The communication during the interrogation period is based on IEC-61334-5-2. The communication during the contention period is based on CEA709.1b and 802.11e.

Communication during the interrogation period follows a master/slave basis, the TC (Transformation Center) acts as master and all the meters as slaves. As a master, the TC is the unique device able to initiate a communication on this period. The aim of this period is to take advantage of the full bandwidth of the network (2400 bps) in order to poll all the devices. As a consequence of this polling process, either interrogation information or synchronization information can be obtained.

Communication during the contention period model a shared medium, this introduces collisions and delays in the end-to-end communication. Collisions are originated by the aggressiveness of the backoff period during the access to the shared medium (this backoff can be configured with the k parameter). Delays are introduced by the backoff period and are needed to access to the medium, this delay will be introduced in every packet's hop. A packet with many hops will be penalized with a large response time.

The medium access during the contention period is achieved through different waiting intervals before the transmission is carried out. This waiting interval is the sum of a fix period and a backoff period. The backoff period is a number of random slots within a congestion window (CW). The value of the fixed period and the congestion window depends on the type of dialog. There are 3 types of dialogs: new dialogs (CIFS), repeated dialogs (RIFS) and acknowledge dialogs (SIFS).

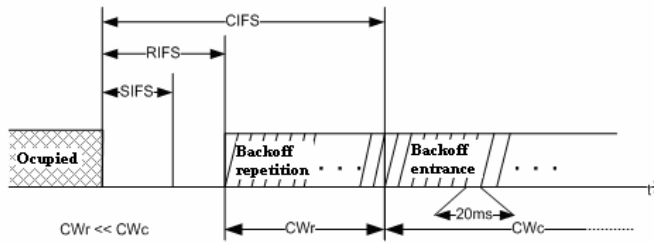


Fig. 1. Scheme of Fixed and backoff periods. The acknowledge dialog only waits the fixed period (SIFS) before its transmission. On the other hand, repeated dialogs wait fixed period (RIFS) and random slots of the CWr window and new dialogs wait fixed period (CIFS) and random slots in CWC window.

The different waiting periods are not in conflict between them because there is a maximum for the different type of dialogs, which can not exceed the fixed waiting period of the next dialog type. As it can be seen in Fig. 1 $(RIFS + CWr) \leq CIFS$. This type of waiting period is based on the 802.11e protocol and its implementation of the HardQoS.

The aim of the contention period is giving flexibility in the meters communications. Originally the contention period was designed for 1Hop dialogs, nevertheless dialogs can begin with more than 1 hop. During this period the meters initiate their associations with de TC.

The definitions of the two periods (backoff and fixed period) explained above require the synchronization of all the devices in the network. Synchronization is very important because the interference between periods is critical. This situation must be avoided, i.e., the interference of a meter in the interrogation period causes the blocking of all the communication mechanism because no collisions are expected to occur and there are no mechanisms to protect against them. The synchronization is achieved sending packets in the contention (KeepAlive) and interrogation (CONTENTION) periods. The KeepAlive packets inform of the remaining slots in the contention period. The CONTENTION packets inform of the number of slots in the interrogation and contention period.

The second MAC layer is a modification of the layer explained above. This MAC layer only implements the contention period, the interrogation period is eliminated. Without the interrogation period there is only one period and type of communications, this removes the needing of synchronization, reducing the traffic management on the network.

Medium Access during contention is slightly different, now the waiting periods are not only based on the type of dialogs; they are also based on the device's type. TC has the minimum waiting time to access to the medium (SIFS) and a meter uses the typical waiting periods depending on the dialog type. Communications began by the TC have priority and as a consequence, the minimum accessing time. Within this situation, a similar implementation of the interrogation period is done, but over the contention period. This priority is needed

because the aim of the communication protocols is polling the entire network. This polling dialog is always initiated by the TC. If the TC had to wait a CIFS period and a random $[0, CWC]$ number of slots, like a meter, the delay introduced by the communication would be inadmissible.

IV. MAC LAYER ANALYSIS

This part is focused on the analysis of the results of each implementation. The results studied hereafter are: the amount of time needed to generate the tree in order to manage the entire network, the different logic topology generated, the protocol adaptation in front of the physical topology changes and the traffic management overhead due to the generation of the logic topology.

A. Tree generation time

The protocols that have been analyzed have the ability to communicate through the PLC network. A logical topology is needed to accomplish this objective. This topology is generated in the network set up, where the amount of time wasted to set up the initial topology is the result of the discussion shown within this section.

The network deployed to make the analysis is constituted of 384 meters, one TC and two branches. The Fig. 2 shows the physical diagram of the deployed network used to collect the results

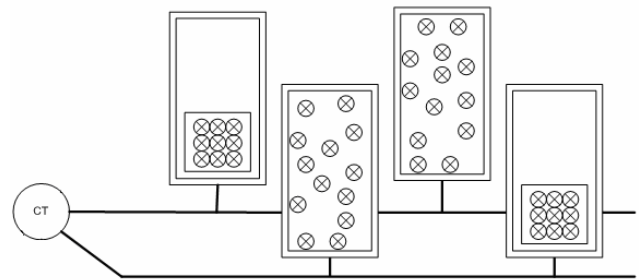


Fig. 2. Network physical diagram deployed.

Fig.3 shows the time elapsed to generate the logical topology and to manage all the nodes in the network. From this analysis two results were extracted: one is for the "Remote reading Project MAC PLC-NB Level" protocol called interrogation and the second is for the contention implementation.

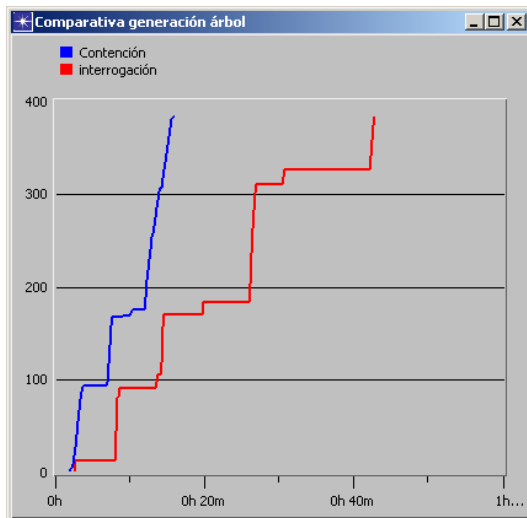


Fig. 3. Time taken to generate the logical topology. In the x axis number of meters in the logical topology (384 is the maximum) is shown. In the y axis the time elapsed in minutes is represented.

The contention implementation has better generation time topology than the interrogation implementation. This is caused by the synchronization required by the communication during the interrogation implementations. This phenomenon can be observed in the Fig.4.

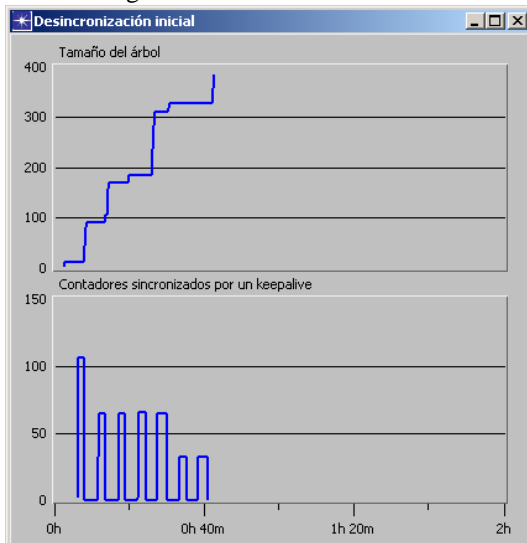


Fig. 4. Delay derived from the network synchronization. The graph on the top of the figure shows the generation topology time during the interrogation implementation. The graph on the bottom part shows the number of partially synchronized counters in the x axis and the time in the y axis. The network synchronization has two steps: the first is to synchronize the network partially (with the reception of a Keep Alive frame) and the second is to synchronize it completely (with the reception of a CONTENTION frame).

This graph illustrates the delay derived from the synchronization. The meters in each level are being synchronized with the network prior to transmit any frame. This waiting time is accumulative to the number of hops needed to reach the meter. The meters in the second hop should wait to the meters synchronization that occurs in the first level. This delay is not introduced by the contention implementation because it does not need any synchronization. The contention implementation takes advantage of the shared

medium.

The contention implementation has another problem. Each time a new dialog is initiated, a fixed and backoff (CW_c) periods must be waited before the transmission of a packet. The backoff period can be configured through the k parameter.

$$CW_c = \frac{2^{18}}{2^k}$$

From the previous formula the k models and the aggressiveness of the medium can be extracted. When k is higher, the contention window is reduced and consequently the backoff period. This reduction models more aggressive medium access, as can be seen in the Fig. 5.

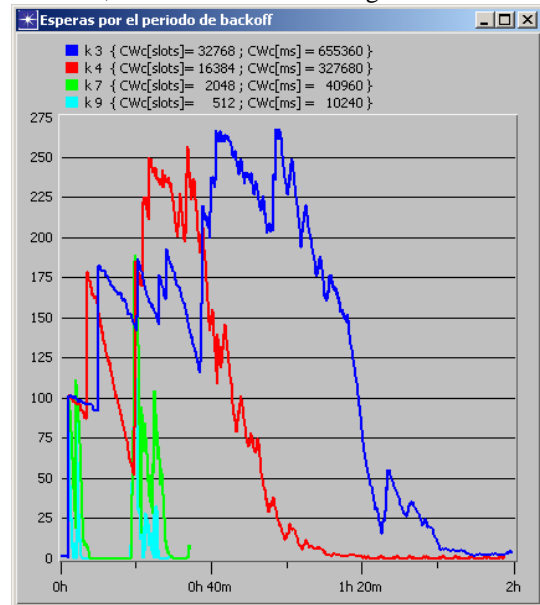


Fig. 5. Aggressiveness of the medium based on the k parameter. In the graph, the y axis is the number of the meter doing a backoff period, and in the x axis the time is shown.

From the Fig.5 the dumping time of the network can be extracted. This time is the period spent to finish all the transmissions in the network. As it can be seen in Fig.5, with a $k = 9$, the backoff period is much better than the backoff period obtained with a value of $k = 3$. The problem of big k increases is the collisions that can be introduced. This adds an overhead to the traffic in the network. The overhead due to packets retransmissions with a k value of 9 is 37,5% over the k value of 3.

B. Logical network

As explained above, to manage all the devices through the physical network a logical topology is created. The logical topology is composed of a tree with its root on the TC. Across the network, some meters need to behave as repeaters, allowing the TC communication with the furthest meters. This topology is used to address all the devices and to determine which of them will behave as repeater or only as meter.

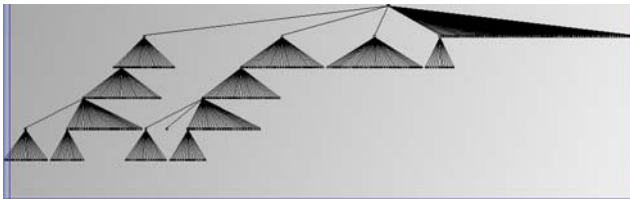


Fig. 6. Logical topology of the interrogation implementation. This logical topology is hierarchical due to the ordered association in levels, first the meter synchronizes and then associates hop by hop.

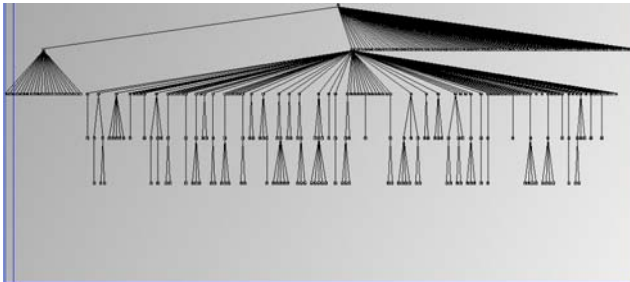


Fig. 7. Logical topology of the contention implementation. This logical topology is more distributed due to the shared medium. In this implementation all the logical structure is generated without any synchronization, this dynamism cauterizes the generated tree.

C. Adaptation to physical changes

The most important problem of these protocols is its dependence of the physical network. The interrogation implementation takes advantage of the numerous configurable parameters that are used to adapt different physical topologies. On the other hand, there is the contention implementation, which does not have much configurable parameters, but the dynamism given by the implementation of a shared medium lets this implementation have a better adjustment to the physical changes, understanding a better adjustment as a little variation in the topology generation time in front of physical changes.

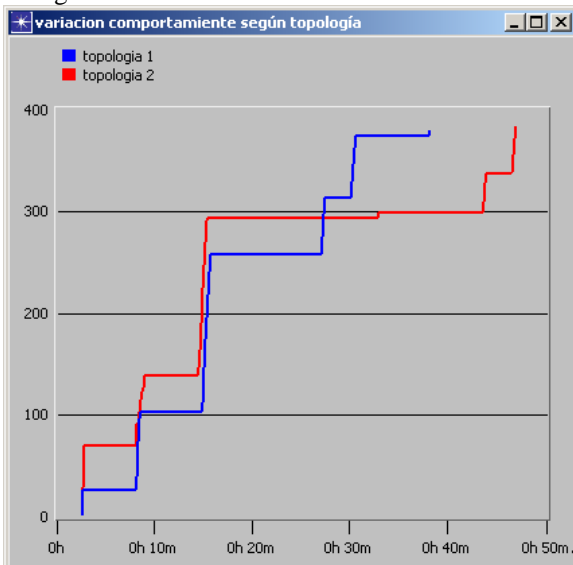


Fig. 8. Variation in the topology generation time due to physical topology changes. This graph represents the variation of time in the interrogation implementation. As it can be seen, there is a variation of 15 to 20 minutes, only provoked by the physical topology changes.

Another physical change that can vary is the attenuation. This parameter heavily affects to the logical topology created, this topology has more hops to achieve the communication with all the nodes in the network. Another effect is the increment of time needed to generate this logical topology. The two implementation responses are different, the interrogation implementation has a greater increment in the logical topology generation time than the contention implementation, but in the end-to-end communication time the interrogation implementation presents a better response. In the next graph can be seen how the attenuation of the medium affects to the logical topology generation time and the number of hops in the network of the both implementations.

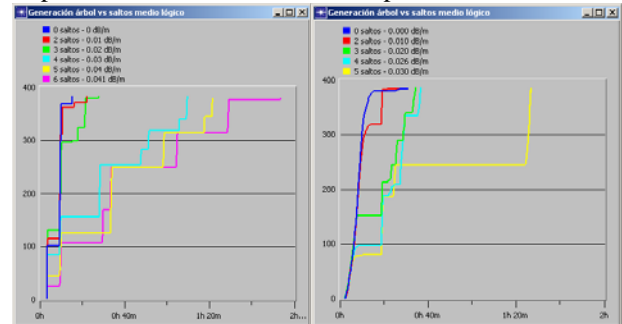


Fig. 9. Time taken to generate the logical topology with each implementation, interrogation and contention respectively. As it can be seen, the interrogation implementation presents a greater increment when the number of hops changes from 3 to 4. On the other hand, the contention implementation presents an increment too, but this is smaller compared with the interrogation increment.

D. Management overhead

The difference between the two previous implementations is that interrogation needed to synchronize the whole network. However the contention implementation does not have this needing. This provokes a bigger consumption of bandwidth in the initial network set up during the interrogation implementation. This is a problem because it reduces the remaining bandwidth for traffic with other purposes such AMR or other type of applications. The contention implementation does not have this problem because it does not need to synchronize the network.

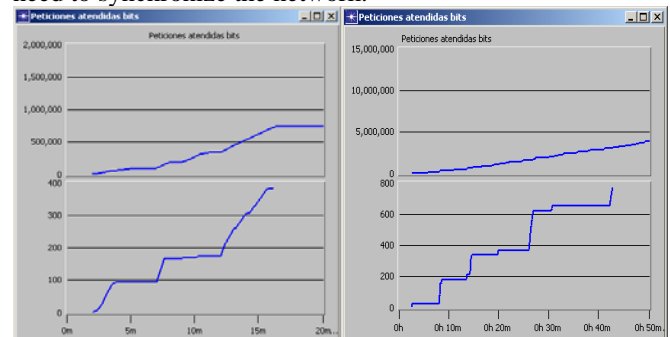


Fig. 10. Bandwidth consumed during the initial network set up. The left part of Fig.10 corresponds to the interrogation implementation and the right part to the contention implementation. The upper graph shows the amount of bits send in the y axis and the time in the x axis. The lower graph shows the generation topology time.

Fig.10 shows how the interrogation implementation has a

greater consumption of bandwidth during the initial set up. The problem of synchronizing the network does not end here, the same problem is repeated during the simulation time because the synchronization traffic needs to be always sent in order to maintain the synchronization. If the meter does not receive synchronization information for a while it considers itself de-synchronized with the network and it will then begin a re-association process.

On Table I the value calculated for the used bandwidth for management traffic purposes is shown.

TABLE I
BANDWIDTH CONSUMPTION WITH MANAGEMENT TRAFFIC

Implementation	Interval (s)	Data transmitted (bits)	Management BW (bps)
Contention	900	750.000	833
Interrogation	2700	3.100.000	1100

The links bit rate used during the simulation is 2400bps. From this table can be extracted that the 45% of the bandwidth on the link is assigned to management traffic in the interrogation implementation, this leaves a little part of the bandwidth to other purpose. On the other hand, the contention implementation utilizes a 35% leaving more bandwidth to other type of traffic.

V. CONCLUSION

The conclusions extracted are divided in two: one part for the interrogation implementation and another to the contention implementation.

The interrogation implementation has an entire period to make polling to the overall network taking advantage of the 100% of the bandwidth of the network. The disadvantage is the definition of two periods of communication, involving a waste of the bandwidth destined to synchronize and manage the network. This implementation has a great scalability through the various configurable parameters, but if the remote reading is the unique task, this implementation presents a big response time to generate the network topology and a heavy dependency with the physical medium.

The contention implementation has only one period of communication, reducing the amount of traffic needed to manage the logical network. This implementation is not scalable because only depends of one parameter, the value of k . But it takes advantage of the shared medium implementation which gives better response time in the generation of the logical topology and better adaptation to the physical medium.

The resume of this conclusion is that the interrogation implementation presents a better scalability and can adopt other task demanded by the network in the future. Besides the contention implementation is great adapted to the remote reading but is not scalable to future demands of the network.

REFERENCES

- [1] Internacional Electrotechnical Comision (2004). IEC-61334. CEI/IEC 1334-1-1: 1995. IHS
- [2] Consumer Electronics Association (2002). Control Network Protocol Specifications. CEA-709.1-B. USA: Technology & Standards Department.