Available online at www.sciencedirect.com
ScienceDirect
Ad Hoc Networks 00 (2019) 1–28

Emergency Aware Congestion Control for Smart Grid Neighborhood Area Networks

Juan Pablo Astudillo León*, Luis J. de la Cruz Llopis

Department of Network Engineering, Universitat Politècnica de Catalunya (UPC), Barcelona 08034 Spain

Abstract

The evolution of traditional electricity distribution infrastructures towards Smart Grid networks has generated the need to carry out new research. There are many fields that have attracted the attention of researchers, among which is the improvement of the performance of the so-called Neighborhood Area Networks (NAN). In this sense, and given the critical nature of some of the data transmitted by these networks, maintaining an adequate quality of service (QoS) is absolutely necessary. In emergency situations, this need becomes even more evident. This article presents a congestion control mechanism, whose parameters are modified according to the network state of emergency. The mechanism also applies a multi-channel allocation technique, together with a differentiation in the QoS offered to the different data flows according to their relevance. These proposals have been evaluated in the context of a wireless mesh networks (WMN) made up by a set of smart meter devices, where various smart grids (SG) applications are sending their data traffics. Each SG application must meet its unique quality of service (QoS) requirements, such as reliability and delay. To evaluate the proposals, some NAN scenarios have been built by using the ns-3 simulator and its 802.11s basic model, which was modified to implement the proposed techniques. Compared with the basic Hybrid Wireless Mesh Protocol (HWMP), Emergency Aware Congestion Control proposal (EA-HWMP), shows significant improvements in terms of packet delivery ratio, network throughput and transit time.

Keywords:
smart grid, neighborhood area networks, wireless mesh networks, hybrid wireless mesh protocol, multi channel allocation, congestion control

1. Introduction

The Smart Grid network has been conceived to improve the management and operation of traditional electricity distribution networks, as well as to provide new services, both to the supplying companies and to their customers [1]. To this end, a data communication network has been incorporated into its infrastructure, which in turn is made up of several sub-networks, each one possibly based on a different network technology [2].

The different smart meters (SM), devices and other utilities present inside homes are interconnected by the Home Area Network (HAN). Selectable technology standards for this HANs could be, among others, IEEE 802.15.4 (Low-Rate Wireless Personal Area Networks, LR-WPAN) or IEEE 802.11 (Wireless Local Area Networks, WLAN). In turn, the HANs are interconnected through the Neighborhood Area Network (NAN), where Power Line Communication (PLC) technologies, or standards such as IEEE 802.15.4g or IEEE 802.11s (Wireless Mesh Networks), can be considered. In terms of ubiquity, WLANs are the closest rival to PLC networks, given that they are both prevalent

*Corresponding author. Tel.: +34-93-401-60-14.
Email addresses: juan.pablo.astudillo@upc.edu (Juan Pablo Astudillo León), luis.delacruz@upc.edu (Luis J. de la Cruz Llopis)

in most homes. Wireless Fidelity (Wi-Fi) is known for its mobility and ease of deployment [3]. Finally, a wired backbone or even another wireless technology standard such as IEEE 802.16 (Wireless Metropolitan Area Networks, WirelessMAN) allows the information exchange between the NANs and the control centers.

To plan, manage and operate a communication network with a highest degree of efficiency, it is essential a deep knowledge of the services that will be provided. The maximum efficiency must be achieved while maintaining the quality of service required by all applications. These considerations are especially relevant when working with Smart Grid, given the critical importance of the power grid infrastructure. The offered services belongs to very different types, and therefore their service quality requirements are also different [4]. Generally speaking, most Smart Grid applications have strong security and reliability requirements. The goal of this paper is to present and evaluate some techniques that allow improving the performance offered by the NANs, when the selected technology to use is based on the IEEE 802.11 wireless mesh networks standard and its Hybrid Wireless Mesh Protocol (HWMP). Specifically, a congestion control mechanism, which takes into account possible emergency situations in the network, and applies also multi-channel allocation and traffic differentiation techniques, is presented. These emergency situations are characterized by a reduction in the network performance, which in turn may be caused by intrinsic (hardware, software, communications protocols, etc.) or extrinsic (weather conditions, malicious agents, terrorist attacks, etc.) failures [5]. This proposal has been evaluated in the context of a smart grid neighborhood area network made up of a set of smart meter devices.

The rest of the paper is organized as follows. In Section 2 we report and analyze the related work. Section 3 presents the multichannel and network congestion control mechanisms. Section 4 evaluates the proposed mechanism. Finally, the conclusions and future works are summarized in section 5.

2. Related work

Several researchers have focused their work on the proposal of new mechanisms, or on the modification of existing ones, with the aim of improving the performance offered by wireless mesh networks in smart grid neighborhood area networks. Authors in [6] presents a performance evaluation and comparison of Optimized Link State Protocol (OLSR) [7] and HWMP (IEEE 802.11s) [8] routing protocols, together with a classification of the main AMI (Advanced Metering Infrastructure) application traffics. Later, in [9] the same authors propose an enhancement of the OLSR protocol by using the combination of different basic metrics. The objective is to offer an adapted quality of service to the different traffics traveling on the network. To this end, they use the combination of different metrics: Expected Transmission Count (ETX), Minimum Delay (MD) and Minimum Loss (ML). They chose Relevant Link Metric Types (RLMTs) for each application, assign different weights to each of them, and use a pruning technique to reduce the number of considered paths to a given destination. In this work, the best link to send each traffic is calculated by means of an AHP (Analytical Hierarchy Process) algorithm.

A modification of the airtime link metric calculation method was presented in [10], in order to improve the network throughput and reliability. The proposed method gives greater relevance to the upstream transmission status (from smart meters to the concentrator), since most data is transmitted in this direction. Although a modification of the path selection mechanism is provided, the results highlight the need for congestion control mechanisms when the network size is increased. In addition, the reliability provided by the HWMP routing protocol and some proposed solutions for its weaknesses are also the main issues addressed in [11] by some of the same authors of [10]. First of all, authors identify those weaknesses, both from the HWMP protocol itself (route instability and route recovery) and from the integration with Smart Grid networks (oversimplified calculation of airtime link metric and the need of traffic differentiation). As in [10], authors propose a modification of the airtime link metric computation and of the path selection mechanism. Now, the possibility of implementing routes reservations is also exploited to reduce packet losses and routing management traffic when a path is broken. Besides, in order to provide a better quality of service to some applications, a delay-tolerant traffic management method based on the concept of delay-tolerant networking is proposed. The modification of the basic HWMP metric is also the key point in [12, 13]. In [12], the packet size and the queuing delay are included in the modified metric, and the frame error rate is computed separately for every application traffic. On the other hand, a new metric oriented to improve the behavior under electromagnetic interferences is proposed in [13]. Some of the same authors have also presented a very good performance analysis for this type of networks in [14].

In [15] a multigate communication network, based on IEEE 802.11s, is proposed for Smart Grids. In order to improve the network performance, the possibility of having more than one node acting as a gateway is presented, together with a real-time traffic scheduling and a multichannel aided routing protocol. To achieve the load balance between gateways, authors propose a heuristic backpressure scheme, where every node evaluates the state of its neighbors before selecting one of them as the best next hop. As authors state, with this scheme there is no need for on-demand routing, but some information (the backpressure metric) must be periodically exchanged between nodes. Another work which considers IEEE 802.11s mesh networks as Smart Grid NANs is presented in [16], where authors propose the HWMP-NQ protocol, a modification of HWMP to ensure the needed QoS of several smart grid traffic types. To distinguish between different applications, the data size and the QoS requirements are considered. The airtime link metric is modified by considering the packet size and the transmission rate, which could increase excessively the needed number of channel measurement. To avoid this, a frame error rate calculation algorithm based on single measurement is also proposed. Besides, the benefits provided by a multi-gateway backup routing scheme are also analyzed. Moreover, to reduce the routing overhead in case of link failures, a modification of the path error mechanism is introduced.

In WMN, there are two types of congestion: intra and inter-mesh congestion. Although there are multiple algorithms to solve intra-mesh congestion, in the context of NAN networks there are no works that focus on congestion control, since they are, in general, aimed to WMN. For instance, a congestion control mechanism for WMN is presented in [17]. Authors have considered that the increase in the waiting time to access the wireless channel also increase the packet delay and then, the resulting queue length leads to congestion. They propose a modification to the default HWMP in order to provide congestion avoidance. They consider that each node monitors its queue length for each flow and they notify to their neighbors when it reaches a specific level through Congestion Control Notification Frames (CCNF). This action allows the neighboring node to calculate an alternative path depending on the queue length and also excluding the congested link.

The implementation of multi-channel in WMNs can be done in two ways: multiple radios on the physical layer (PHY) or using the channel switching capability of the device. The proposals and works in [18, 19, 20, 21, 22] describe techniques for channel assignment, multiple beam-antennas and multiple-radio routing metrics. However, this concept, together with congestion control techniques, has not been fully investigated in NAN networks when the WMN is implemented as the technology for data communications. For instance, in a previous work [23] a basic congestion control mechanism for WMN is proposed, which works together with a multi-channel allocation scheme. In this work, two traffic types have been defined (priority and non-priority), and the congestion control mechanism discards non-priority applications when a given channel utilization factor value is exceeded. Besides, in order to reduce the network congestion, two different channels have been used for transmitting the different NAN applications.

In this work, we put together and evaluate our proposals for multi-channel allocation and for congestion control, considering the different service quality needs of the different applications. The congestion control mechanism takes into account if the network is in a state of emergency. For this, three network emergency states have been defined: normal, medium or high. Each of these states can be activated manually or automatically. For automatic operation, the network nodes periodically measure different performance parameters, and alert the rest of the nodes (by means of special management frames) in case of detecting anomalous situations. The presented techniques are executed individually in every node, and do not significantly load the nodes CPU, which is advisable if we take into account that in many cases these devices are built on a large scale and at low cost, and so they have limited resources.

3. An Emergency Aware Congestion Control mechanism for HWMP

The implementation of the HWMP protocol integrates these main processes: Route Management, Data Queue and Route Assignment [24]. In order to improve the performance of the basic protocol, in this paper four specifics mechanisms, which work collaboratively, are proposed, implemented and evaluated: traffic differentiation, multi channel allocation, congestion control and emergency system. Figure 1 shows the structure of the modified HWMP, with the new modules and their relation with the basic ones, and Tables 1 and 2 present the definition of the variables and functions for the proposed emergency aware congestion control mechanism (EA-HWMP).

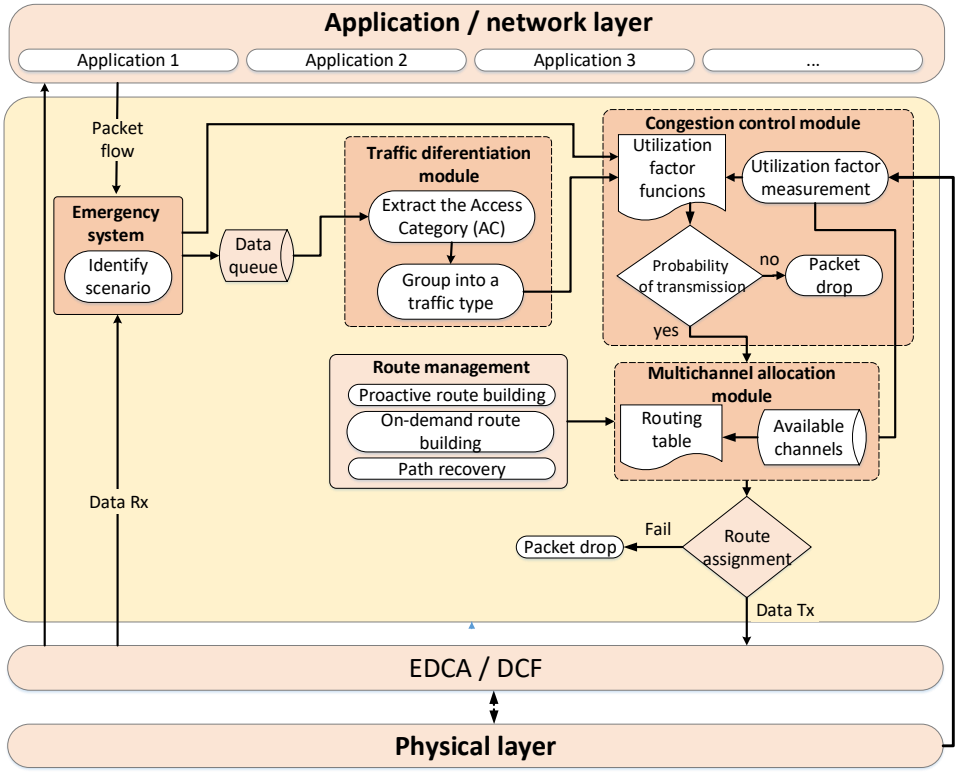


Figure 1: Structure of the emergency aware congestion control mechanism (EA-HWMP).

Table 1: Definition of the variables for the emergency aware congestion control mechanism (EA-HWMP).

Parameter	Description
N_c	Number of available data channels.
ρ	Channel utilization factor for each data channel.
ρ'	The previous value of ρ.
s_ρ	Current sample of the physical channel state.
ω	The value of $\omega(\omega \in [0,1])$ defines the importance of s_ρ with respect to the past values.
f_r	Data frame (NAN application).
ρ_T	The sum of ρ of all available data channels.
t_T	NAN applications are classified into four traffic types.
ccf	Congestion control functions.
P_T	Transmission probability based on the result of ccf.
E_S	Emergency situation (normal, medium and high).
s	Source mac address.
d	Destination mac address.
AC	EDCA access categories (voice (VO), video (VI), best effort (BE) and background (BK)).
TTL	Time-to-live.
ρ_{th}	The maximum threshold of ρ allowed per channel.
ch	Data physical channel.

Table 2: Definition of the functions for the emergency aware congestion control mechanism (EA-HWMP).

Function	Description
isStateBusy	Measures the physical channel state (busy: 1, iddle: 0).
mapTraffic	NAN applications are mapped to the four EDCA access categories.
shouldTransmit	Depending on the ρ_T, ccf and E_S values, the frame will be pass to the multichannel allocation module.
congestionControl	Congestion control mechanism (Algorithm 1).
channelAllocation	Data frames are assigned to a specified channel based on the value of ρ_{th} (Algorithm 3).

Different NAN applications are (re)transmitted through the NAN network, as well as routing and emergency messages. First, the data messages (NAN applications) are grouped into four traffic types according to their priority, where the traffic type 1 corresponds to the NAN applications with the higher QoS requirements, while the traffic type 4 represents the applications with less QoS needs. Second, different emergency messages are used to characterize different anomalous situations present in the smart grid (weather conditions, malicious agents, terrorist attacks, hardware or software failure, etc.). Besides, emergency messages modify the operation of the congestion control module. This module basically gives a higher probability of transmission to priority traffic types in situations of network congestion, and this probability will increase or decrease according to the current emergency state (normal, medium and high) of the smart grid. Finally, a multichannel allocation module is also implemented, which assigns a dedicated channel for the control traffic and the rest of channels are assigned to transmit the NAN applications. These modules will be explained in greater detail in the following sections.

3.1. Route management

This module is responsible for computing and updating the paths through a proactive or an on-demand path-building mechanisms. When a new data frame arrives at this module from the application or physical layer, it is immediately stored at the HWMP queue. If the frame must be forwarded, the mesh STA selects the best path for its transmission. For this purpose, the HWMP checks the destination address and looks up the next hop address in the routing table, previously calculated by the path-building mechanisms. If a path is available, the mesh STA transmits the frame by using the medium access mechanism. On the other hand, if there is not a route to the destination, the path discovery mechanism is activated. For this purpose, a Path Request (PREQ) message is broadcast from the source to the whole network, and when this message reaches the intended destination, this node replies with an unicast Path Reply (PREP) message to the PREQ originator node by using the best path (lower metric) [24]. Finally, in the case of one or more unreachable destination(s), the mesh STA drops the frame and transmits control messages such as path error (PERR) in order to invalidate the whole path. This message is sent to all traffic sources that have a known active path to the destination(s). The active forwarding information associated with the unreachable destination(s) should no longer be used for forwarding [8]. It must be kept in mind that different channels have been used for control and data traffic, where just one channel is assigned to the control traffic (routing and emergency messages), and the rest of the available channels are assigned to transmit the data frames.

3.2. Traffic differentiation module

As will be detailed in section 4, in this work the different applications (data traffic flows) that are transmitted through the network are classified into four traffic types. Data packets arriving from the network / application layer are labeled with a specific access category. The objective is to map the traffic types according to the Enhanced Distributed Channel Access (EDCA) categories. For example, the traffic type 1, which has the highest QoS requirements (e.g., Demand Response applications), is mapped to the voice (VO) access category, while the traffic type 4, which has the lowest QoS needs (e.g., Meter Reading), is assigned to the background (BK) access category. The proposed scheme does not modify the medium access mechanism, since the access categories are used to identify the NAN applications and group them into different traffic types according to their priorities.

3.3. Congestion control and emergency system modules

The network congestion mechanism (Algorithm 1) is based on the value of the channel utilization factor (ρ) . This parameter is measured by the mesh STA itself. The possible values are channel busy or idle. However, in

our practical implementation, these values are smoothed to avoid undesired oscillations. For this, an exponentially weighted moving average (EWMA) is used, where the smoothing factor (ω) was set to 0.0005. The ρ measurement is performed before the multi channel allocation takes place. This is because the selection of the channel for a frame to be forwarded will depend on the access category (traffic type (t_T)) and the result of the network control congestion mechanism at that precise moment.

Algorithm 1: Congestion control algorithm.

Input: data frame (f_r) (NAN application)
Output: According to the channels utilization factor functions, the frame must be transmitted or not.

for $i \leftarrow 1$ **to** N_C **do**
  $s_{\rho_i} \leftarrow \text{isStateBusy}(ch_i)$
  $\rho_i \leftarrow \omega \cdot s_{\rho_i} + (1 - \omega) \cdot \rho'_i$
$\rho_T \leftarrow \sum_{i=1}^{N_C} \rho_i$
$t_T \leftarrow \text{mapTraffic}(f_r)$
$P_T \leftarrow \text{ccf}(t_T, \rho_T, E_S)$
if shouldTransmit(P_T) **then**
  return **true**
else
  return **false**

The proposed congestion control mechanism is based on the definition of a congestion control function that assigns a transmission probability (P_T) to each value of the utilization factor. In this way, each time a node receives a packet to be (re)transmitted, this transmission will be effectively made with probability P_T, or the packet will be discarded with probability $(1 - P_T)$. On the other hand, since it is desired to differentiate the quality of service offered to the different types of traffic, it is proposed to use a different congestion control function for each of them, as shown in Figure 2. In addition, since the proposed mechanism is multi-channel (with a maximum of N_C available channels), the sum of the utilization factors of all available channels will be taken into account ($\rho_T = \rho_1 + \cdots + \rho_{N_C}$). Thus, in situations of network congestion (high values of ρ_T), traffic types with lower needs ($t_T = 3$ or $t_T = 4$) will be more likely discarded. It must be kept in mind that the applications assigned to traffic types with lower priority must be those that are less sensitive to possible packet losses (for example, meter reading applications that repeat and periodically retransmit the power consumption measurements).

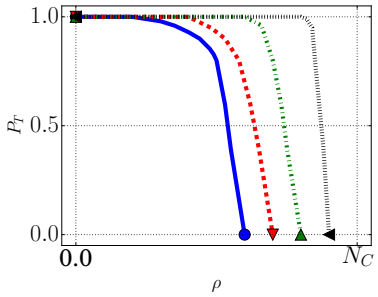
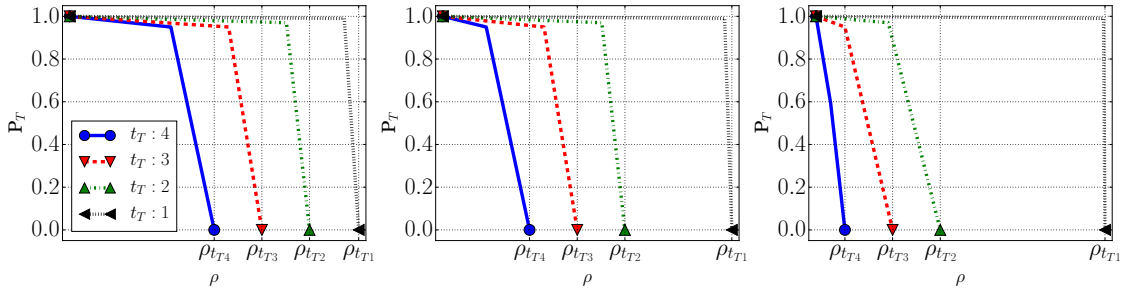


Figure 2: Congestion control function.

The congestion control mechanism works collaboratively with the emergency system module. The objective of the emergency system is to increase even more the probability of transmission of higher priority traffic in medium or high emergency situations. For this, NAN applications with lower priority are discarded at a higher rate in the time intervals in which the emergency occurs, and those with higher priorities are provided with an even better QoS. The congestion control functions, and the channel utilization factor thresholds, for each traffic type and for each emergency situation (E_S), are shown in Figure 3 and Table 3 respectively. On the other hand, the dissemination of emergency situations is done through broadcast messages, since all the nodes must know the situation. Each message contains the address of the originator node and the emergency situation, such as normal, medium or high. Finally, these messages are propagated in the network through a dedicated physical channel, to avoid high delays in congestion situations.



(a) normal. (b) medium. (c) high.

Figure 3: Congestion control functions for different emergency situations.

Table 3: Channel utilization factor thresholds for each traffic type and for each emergency situation.

	Emergency situation		
	Normal	**Medium**	**High**
$\rho_{t_{T1}}$	2	2	2
$\rho_{t_{T2}}$	1.66	1.26	0.86
$\rho_{t_{T3}}$	1.33	0.93	0.53
$\rho_{t_{T4}}$	1	0.6	0.2

After the data frame is classified according to the traffic type (traffic differentiation module), a random number is generated between 0 and 1, and if this value is below the transmission probability (P_T), the data packets are passed to multi-channel allocation module to be transmitted. Otherwise, the data packets are discarded.

3.4. Route assignment and multi channel allocation

The general route assignment tasks performed by the network nodes every time they have to (re)transmit a packet are detailed in Algorithm 2. First, the node extracts the following parameters from the packet header: source node, destination node, access category, and time to live. Then, the algorithm looks up if there is an available route. In the affirmative case, the next hop node is obtained by means of the route selection algorithm by taking into account the destination node. After, the congestion control mechanism computes if the frame should be transmitted or not based on the emergency situation (E_S) and the network congestion (ρ_T and ccf). Finally, the transmission is assigned to a specific channel. In the case that there is no route, the packet is queued, and the path discovery mechanism is activated. This mechanism tries to obtain the route a fixed number of times, and if that threshold is exceeded, the route to that destination is considered invalid and the packet is eliminated.

Algorithm 2: Route assignment.

Input: NAN application (f_r)
Output: Forward the data to the next hop depending on the multiple channels available at the node.

```
receive_data(f_r)
[s, d, AC, TTL] ← read(f_r)
[next_hop, isThereRoute] ← RouteSelection(d)
if isThereRoute then
    if congestionControl(f_r) then
        ch_d ← channelAllocation(f_r)
        send(f_r, next_hop, ch_d)
    else
        drop(f_r)
    return
else
    if shouldInitiatePathDiscovery(d) then
        lastSQN ← getLastSQN(d)
        preq ← createPreq(lastSQN, d)
        sendPreq(preq)
    queuedPacket(packet)
```

The multi channel allocation module (Algorithm 3) is composed of two parts: the routing table created by the path-building mechanisms (proactive or on-demand) and the number of physical channels available in the current mesh STA. The purpose of this module is to select the next hop address to forward a data frame, and depending on the result of the network congestion module and the value of ρ of each channel, the transmission will be assigned to an specified physical channel.

Algorithm 3: Multichannel allocation algorithm.

Input: Number of available data channels.
Output: Assigned channel for transmission

```
channel ← 1
for ch ← 1 to N_C do
    if ρ_i < ρ_th then
        return ch
    else if i == n then
        return noChannel
```

If the output of the congestion control module indicates that the frame should be passed to the MAC sub-layer to be transmitted, the next process is to select the physical channel for the transmission. Our proposal for multichannel allocation is based on the use of the least possible number of channels at any given time. For this, the utilization factor of each channel (ρ_i) is taken into account. By default, the data packet is assigned to the data channel number 1, if and only if the value of ρ for this channel is below a certain threshold ($\rho_1 < \rho_{th}$). Otherwise, the transmission is assigned to channel number 2, and if this channel is also busy ($\rho_2 > \rho_{ch}$), the transmission is assigned to the next channel and so on up to the maximum number of available channels (N_C). In addition, if the last available channel is also busy, the data packet will be discarded. Finally, to avoid abrupt fluctuations due to channel changes, a hysteresis cycle is taken into account around the central value of ρ_{th}.

4. Experimental evaluation

Figure 4 shows the scenario for the evaluation of our proposal, where various applications (traffic types) are transmitted upstream from the smart meters (SM) towards the data concentrator, and downstream from the concentrator towards the smart meters. The network scenario consist on a grid topology, where the number of nodes in the grid will be a variable parameter in the simulation runs, and the data concentrator is positioned at the bottom left corner. In

this scenario, home users transmit different types of traffic, for instance, periodic billing data (meter reading), electric vehicle (EV) charging information and other applications. On the other hand, it is possible to transmit demand response information from the control center to adjust, among other possibilities, the consumption peaks of households to the time periods in which the price of electricity is lower. The experiments consider that these applications runs simultaneously on all smart meters.

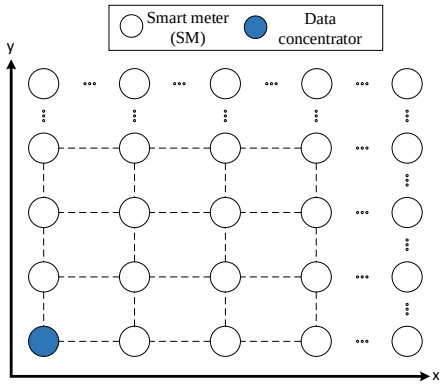


Figure 4: Scenario under consideration.

Table 4: Traffic types for different NAN applications.

Traffic type	Applications	Packet size		Packet interval		EDCA
		Length (Bytes)	Distribution	Interarrival time (secs)	Distribution	
1	Demand Response, Outage Management	200	Exponential	0.1	Exponential	Voice (Highest priority: 1)
2	Video surveillance, Overhead Transmission Line Monitoring, Substation Automation systems (SASs)	200	Exponential	0.1	Exponential	Video (Priority: 2)
3	Home Energy Managament (HEM), Electric Vehicles (EVs) Charging	400	Deterministic	0.1	Deterministic	Best Effort (Priority: 3)
4	Meter Data Management	400	Deterministic	0.1	Deterministic	Background (Lowest priority: 4)

As previously mentioned, the different applications, current or future, that can be transmitted over the NAN, have been grouped into four traffic types according to their quality of service requirements. Every traffic type is in turn mapped into an EDCA category. Table 4 shows this classification, which also shows the distributions and average values selected for the packet size and interarrival time. For traffic types that group applications which generate constant size packets at regular time intervals, the distributions have been considered as deterministic. On the other hand, for the traffic types generated by different types of events or by variable rate applications, an exponential distribution has been considered, which can be better adjusted to the combination of this type of applications. In addition, to evaluate the network performance under stress situations, the packet generation rates have been selected relatively high for all types of traffic.

To evaluate the performance of the proposed mechanisms, the ns-3 simulator [25] was chosen. This tool includes the basic 802.11s model, which was modified to build the traffic differentiation, congestion control, multichannel allocation and emergency mechanisms, as previously explained in Section 3. The simulation setup illustrates the bi-directional flow of information between smart meters and the data concentrator using the WMN as the communication medium. Table 5 presents the different values used for the application, MAC and physical layers.

For each grid size (number of smart meters), different simulation runs have been carried out with different random seeds in order to obtain confidence intervals for the chosen performance measures: packet delivery ratio, throughput, network transit time, and channel utilization. To ensure the network topology shown in Figure 4, we chose 80 meters as the grid distance between nodes. With this value and the propagation model parameter values, each node is only able to establish connections with the neighbors located on its sides.

The IEEE 802.11 standard defines the methods to initiate, maintain, and close the bidirectional links between mesh STAs and also establishes by default the Hybrid Wireless Mesh Protocol and the airtime link metric. Table 5 also presents the parameters configured in the simulator for the MPM and HWMP protocols, where, among others, the following variables are defined: maximum thresholds to consider invalid links, maximum number of neighbors (peer links) allowed, the on-demand and proactive modes of HWMP, lifetime of the reactive and proactive routing information, time interval between two successive proactive PREQs, and the conditions to indicate a route as unreachable. As mentioned, nodes must be allowed to establish links only with the neighbors at their sides. To reinforce this, the maximum number of peer links per node was set to four. On the other hand, the 802.11s model implemented in the ns-3 simulator considers a link as not valid if the consecutive number of lost beacons achieves a configurable threshold (*maxBeaconLoss* in Table 5). A value of 20 lost beacons was selected for this parameter. In addition, when a station is unable to transmit to its peer a number of successive data frames, the ns-3 implementation by default closes their peer link. This parameter and the other variables for the MPM and the HWMP were configured with their default values. These selections do not affect the performance evaluation carried out, since the values are the same for both compared protocols. Finally, the 802.11a mode was selected as the physical layer. Except for the number of data channels and their frequencies (which have been defined in this proposal), well-known values were chosen for the rest of the physical parameters, which are used in most smart grid NAN simulations.

Table 5: General simulation parameters.

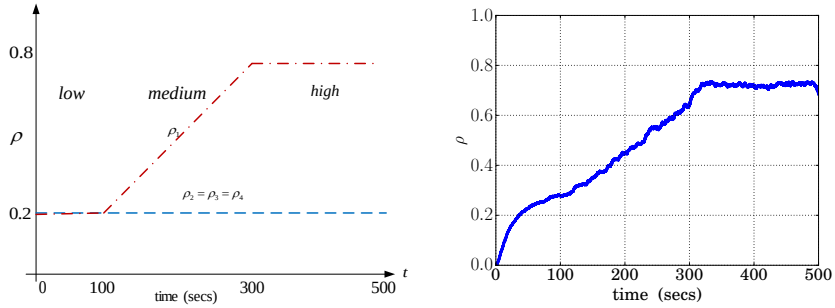
	Variable	Description	Value
Application parameters	simulator	Network simulator.	ns-3.28
	numNodes	Number of nodes.	from 9 to 36
	distanceNodes	Distance between nodes.	80 m
	simTime	Simulation time.	500 s
	tranportLayer	Tranport layer.	UDP
	randomGenerator	Random number generator	MRG32k3a
Hybrid Wireless Mesh Protocol (HWMP) parameters	pathMode	Path selection mode.	On-demand and Proactive
	maxQueueSize	Maximum number of packets we can store when resolving the route.	255
	maxPREQretries	Maximum number of retries before we suppose the destination to be unreachable.	5
	reactivePathTimeout	Lifetime of reactive routing information.	5.12 s (Case 1) 0.512 s (Case 2)
	proactivePathRootTimeout	Lifetime of proactive routing information.	5.12 s
	proactiveRootInterval	Interval between two successive proactive PREQs	1.024 s
Mesh Peering Management (MPM) protocol parameters	maxRetries	Maximum number of retries.	4
	maxBeaconLoss	Maximum number of lost beacons before the link will be closed.	20
	maxPeerLinks	Maximum number of peer links.	4
	maxPacketFailure	Maximum number of failed packets before the link will be closed.	5
Physical layer parameters	phyLayer	Wireless physical layer.	802.11a
	controlChannelNumber	Number of control channels.	1
	dataChannelNumber	Number of data channels.	3
	controlChannelFreq	Frequency of control channel.	5200 MHz
	dataChannelFreq	Frequency of data channels.	5220 MHz 5240 MHz 5260 Mhz
	ρ_{th}	The maximum threshold of ρ per channel	0.5
	propagationDelay	Maximum propagation delay.	3.333 s
	propagationModel	Exponent: the exponent of the path loss propagation model.	3
		ReferenceDistance: the distance at which the reference loss is calculated (m).	1 m
		ReferenceLoss: the reference loss at the reference distance (dB) (the default is Friis at 1 m with 5.15 GHz).	46.667

In the following sub-sections, two simulation scenarios (congestion and emergency) are implemented and evaluated in terms of packet delivery ratio, network transit time, throughput and channel utilization factor measurements. The first three parameters highlight the advantages obtained when the multichannel allocation and congestion control mechanisms are implemented, while the last one measures the channel effects when using multiple channels for the transmission of data and control frames. The ns-3 simulator provides tools for the analysis of results, but they are mainly focused on protocols that operate at the network layer. Given that our mechanisms are based on the protocol HWMP that works at the link layer, a new tool to evaluate the results was programmed.

4.1. Congestion control scenario

First, the behavior of the proposal is evaluated according to different network load situations, without taking into account the emergency mechanism. For this, the packet rate generation of traffic types 2, 3 and 4 remains constant,

while the rate of traffic type 1 (the highest priority traffic) is increased along the simulation. This implies a channel utilization factor by each of the traffic types as shown in Figure 5a. The precise value of the total channel utilization factor measured by one of the network nodes during the simulation is shown in Figure 5b. As can be seen, in the "low network load" stage all the NAN applications have a low packet generation rate in order to not saturate the network. After a period of time, applications that belongs to the traffic type 1 begin to increase the number of the data flows ("medium network load"). In the last stage ("high network load"), the value of ρ_1 remains constant again. As previously said, in order to isolate and validate the traffic differentiation achieved by the congestion control mechanism, without considering the network emergency situation, the network state has been set as normal (see Figure 3a) for all this set of simulations.



(a) target ρ.

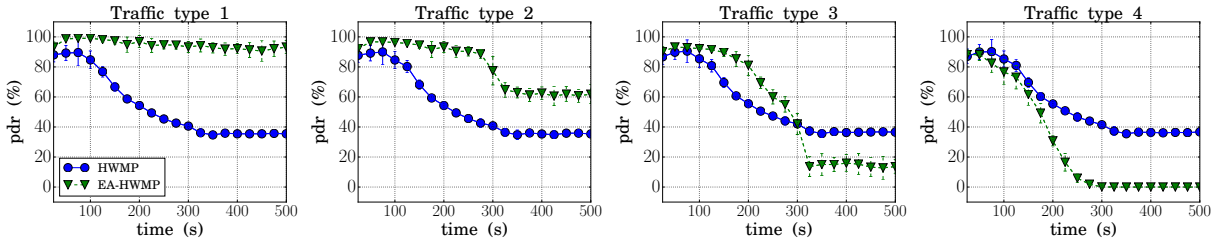
(b) measured ρ.

Figure 5: Traffic generation for the different NAN applications.

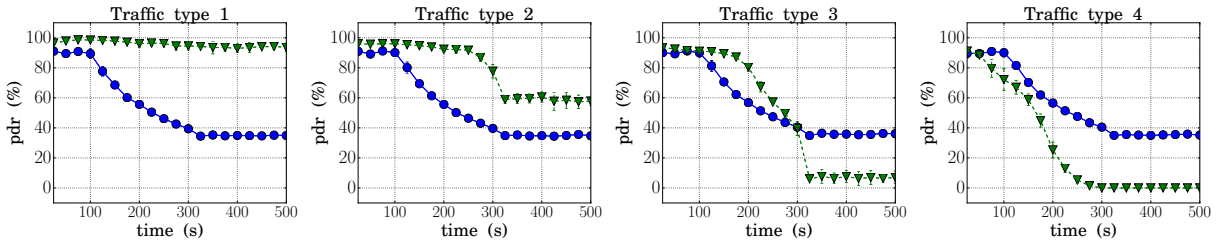
4.1.1. Packet delivery ratio and network throughput

The packet delivery ratio (PDR) describes the relationship between the number of successfully received packets and the total number of transmitted packets. On the other hand, the throughput represents the number of bits per second received correctly, and is a performance parameter that complements the PDR. The benefits obtained in terms of PDR and throughput are presented in two ways. First, the HWMP and our proposal (EA-HWMP) are compared taking into account the evolution of the PDR and the throughput over time. Second, the average values are compared for different network sizes.

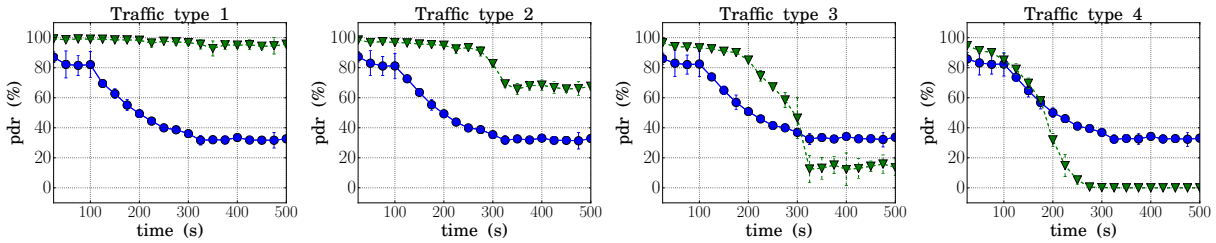
As said, in order to check the correct behavior of the congestion control mechanism, the temporary evolution of the PDR and the throughput (and their 95% confidence interval) are shown in Figures 6 and 7 respectively, in a different plot for each traffic type. The network size chosen to show these results is 16 nodes, and three HWMP configurations have been configured. As can been observed in Figure 6, with the basic HWMP protocol the behavior is the same for the three HWMP configurations and for all traffic types, with a decreasing PDR as the network load grows (Figure 5). However, EA-HWMP prioritizes the transmission of traffic types with higher QoS needs when the network load grows. On the other hand, in Figure 7, the throughput (bits per second correctly received) is compared with the target throughput (bits per second transmitted) for both protocols. Obviously, the target throughput is the same regardless of whether the protocol used is HWMP or EA-HWMP. Nevertheless, the throughput is always higher when the protocol used is EA-HWMP for priority traffic types. In this case, when a frame is ready to be forwarded, the mesh STA looks up in its routing table the next hop address and depending on the congestion control functions (Figure 3), which are based on the sum of ρ of all available data channels and the traffic type, a transmission probability is calculated. As it was explained, the congestion control functions give more importance to traffic with greater quality of service requirements in situations of network congestion. Then, if the frame is selected for transmission, a specified channel will be assigned considering the maximum value of ρ allowed per channel. That is, if the ρ threshold (ρ_{th}) is exceeded, the next available channel will be assigned to transmit the frame. In addition, Figure 7, shows how the delivered throughput for traffic type 1 is increased in the "medium network load" stage, while the delivered throughput for the other NAN applications are maintained with same packet generation rate, it complements the traffic pattern configured in the application layer (Figure 5).



(a) On-demand mode. Reactive routing information lifetime: 5.12 s.



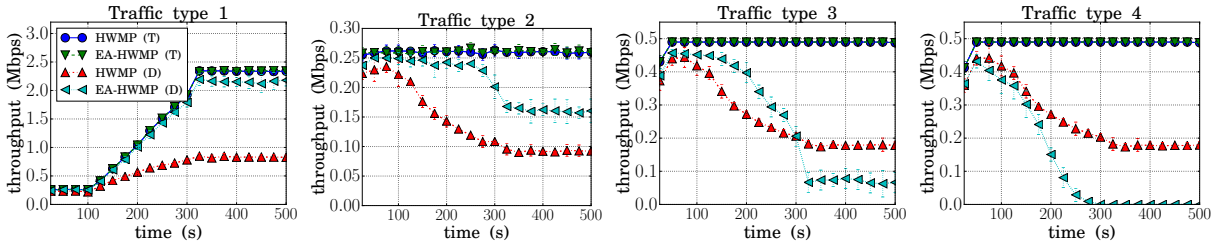
(b) On-demand mode. Reactive routing information lifetime: 0.512 s.



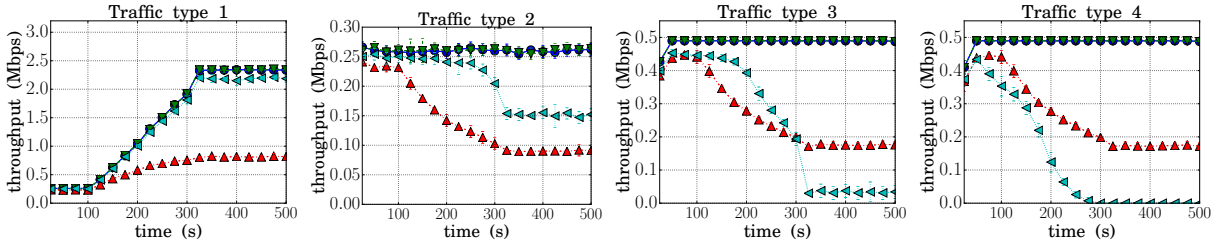
(c) Proactive mode. Proactive routing information lifetime: 5.12 s.

Figure 6: Packet delivery ratio (temporary evolution, grid size: 16 nodes).

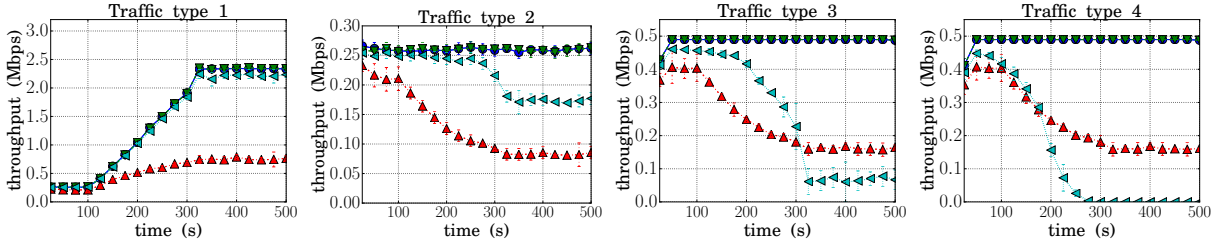
Besides, Figure 6 and 7 show the same results for the on-demand and proactive modes when working in a static scenario. It must be kept in mind that these two modes differ mainly in the mechanism to disseminate the PREQ messages. In the on-demand mode, PREQ messages are transmitted when a route to a destination node expires (*reactivePathTimeout* from Table 5). While in the proactive mode, these messages are sent based on the time interval value configured between two successive proactive PREQs (*proactiveRootInterval* from Table 5). Therefore, modifying the *reactivePathTimeout*, *proactiveRootInterval*, and *proactivePathRootTimeout* variables does not modify the paths calculated by the algorithm. In order to reduce the amount of network resources used to transmit routing messages, the following results will be shown for the on-demand mode, and when the *reactivePathTimeout* variable is set to 5.12 s.



(a) On-demand mode. Reactive routing information lifetime: 5.12 s.



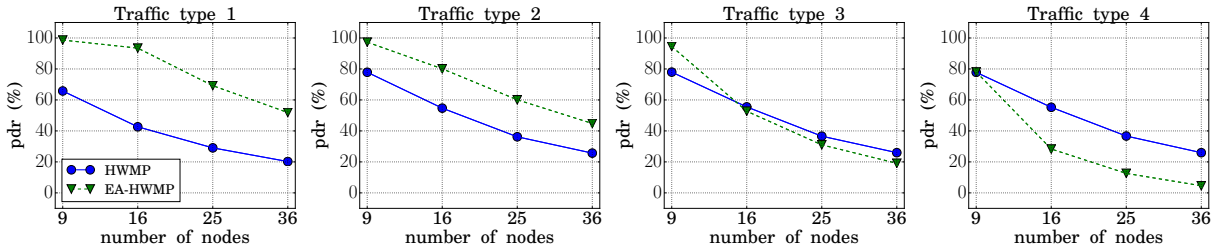
(b) On-demand mode. Reactive routing information lifetime: 0.512 s.



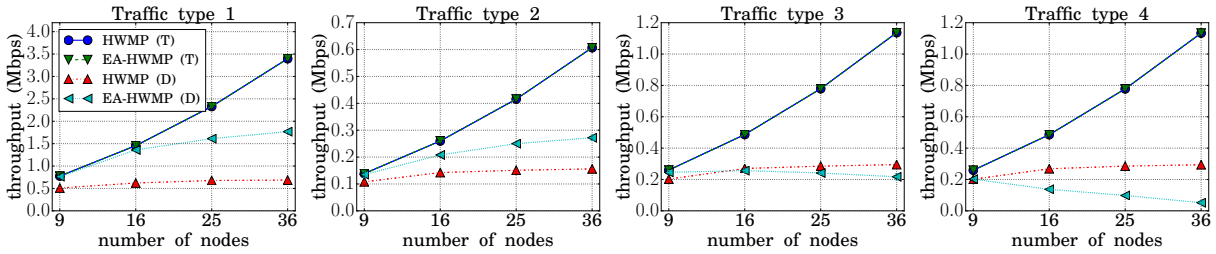
(c) Proactive mode. Proactive routing information lifetime: 5.12 s.

Figure 7: Network throughput (temporary evolution, grid size: 16 nodes).

The second set of results is shown in Figure 8, where the average PDR and throughput (and their 95% confidence interval) for different network sizes (from 9 to 36 nodes), and for the four traffic types under consideration, is presented. It can be observed how, as the network size is increased, it becomes more congested and so the PDR decreases for all traffics. However, this decrease is smaller with EA-HWMP for priority traffic types. Of course, the price to pay is a greater decay in the PDR for lower priority traffics, and this decrease is even greater when the number of nodes is increased in the simulations. Therefore, there is a trade-off to guarantee a targeted PDR for priority traffic at the expense of the loss of a percentage of non-priority traffic. As already mentioned, only those applications which are less sensitive to packet loss must be included in lower priority traffic types. Finally, as Figure 8b shows, the target throughput increases with the size of the network, since a greater number of nodes implies a greater volume of transmitted traffic (keep in mind that all the nodes transmit equally). Again, when EA-HWMP is used, for higher priority traffics the difference between the value of the target and actual throughput is lower, at the expense of a greater difference for lower priority traffics.



(a) Packet delivery ratio.

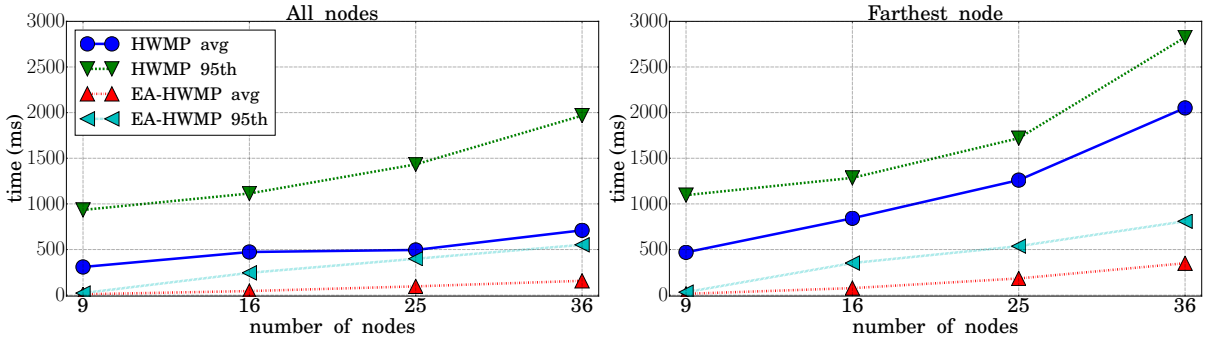


(b) Network throughput.

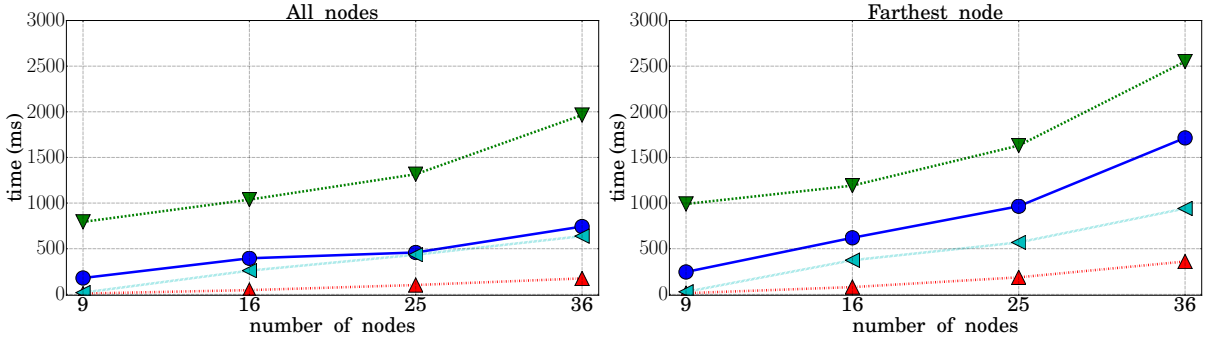
Figure 8: Packet delivery ratio and throughput for different network sizes. Reactive Mode. Reactive routing information lifetime: 5.12 s.

4.1.2. Network transit time

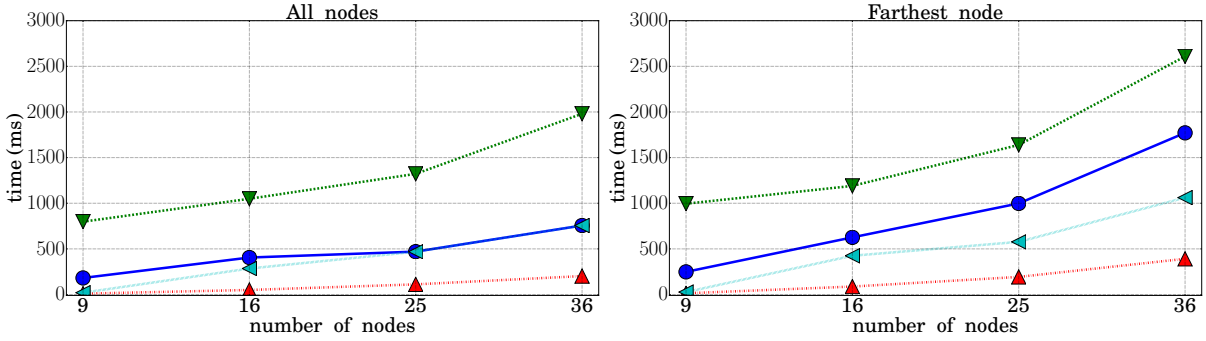
Given the critical nature of some applications that transmit their data through the Smart Grid NAN, it have been considered of importance the analysis of the percentiles of the transit time in conjunction with the average value. In addition, given the size of these networks, we have also considered important to offer, along with the average values for all the network nodes, the values obtained for the farthest smart meter from the concentrator, since these are the values that should be taken into account when planning the network. Figure 9 compares the value of the average value and 95th percentile for the HWMP and EA-HWMP cases. As can be seen, these values are always lower (for all network sizes and for all types of traffic) when using the techniques proposed in this article. In this figure, a significant improvement is observed in the average and percentile values obtained. In the farthest node case, the improvement is really substantial, with an important reduction of the percentile values for large network sizes.



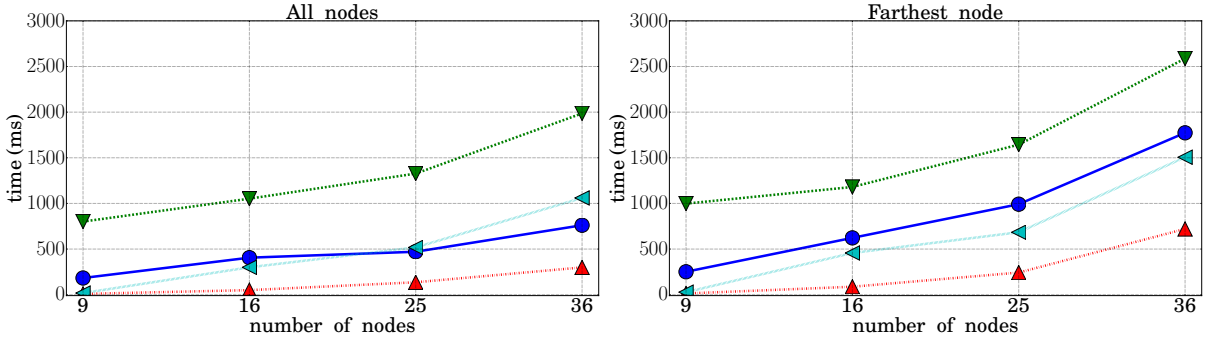
(a) Traffic type 1.



(b) Traffic type 2.



(c) Traffic type 3.



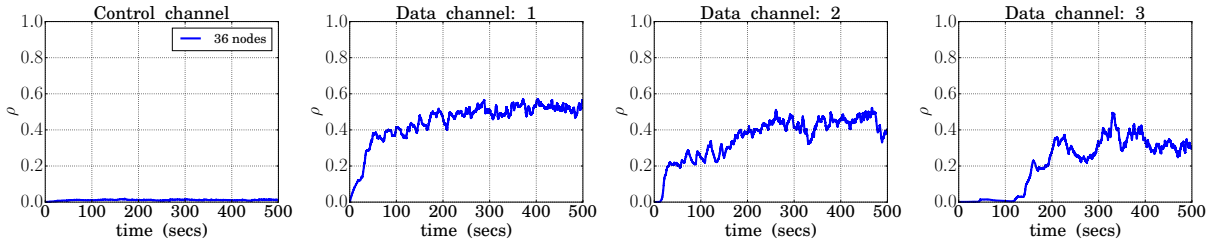
(d) Traffic type 4.

Figure 9: Network transit time.

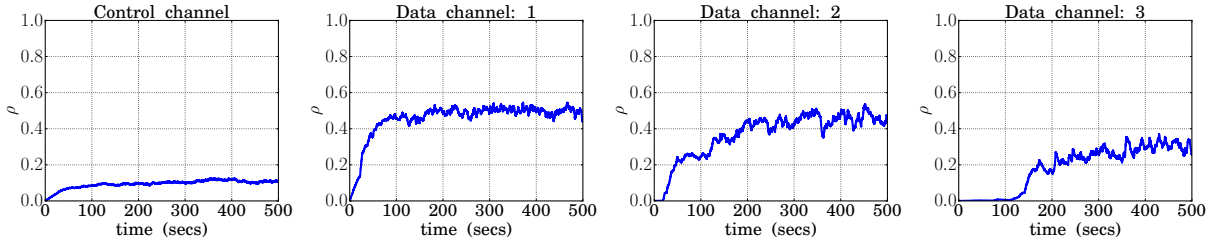
4.1.3. Channel utilization factor

The possibility of having multiple channels implies an increase in the number of successfully transmitted packets to the destination. EA-HMWP assigns the transmission of frames to the next available channel when the following situations are true. First, the probability of transmitting the frame is calculated taking into account the congestion control functions defined for each traffic type. Second, if the frame will be effectively transmitted, the transmission is assigned to the first available data channel (channel 1 by default). However, if the ρ of this channel is above the accepted threshold for that channel, the transmission will be assigned to channel 2 and so on up to a maximum limit of three data channels.

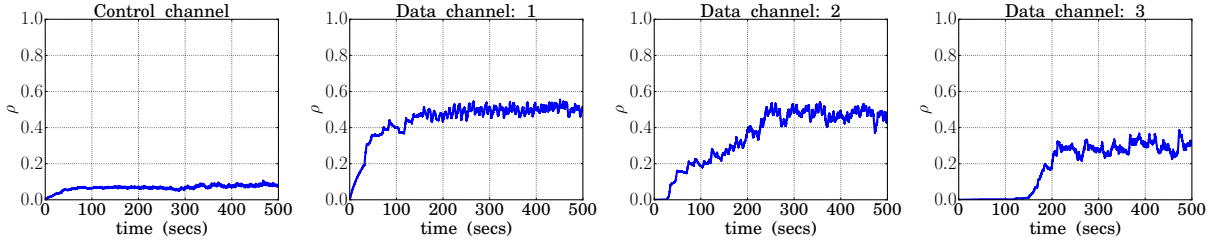
Figure 10 shows the utilization factor for the four available channels: three data channels, as mentioned above, plus one control channel. The control channel is used exclusively for the transmission of routing and emergency signaling packets, as will be explained in the next section, and so its utilization factor is very low. However, the control channel utilization factor is greater when the interval time between two successive PREQs is reduced (Figures 10a, 10b and 10c). Regarding the data channels, it can be observed that the ρ value does not achieve high values (it is always below the configured threshold), and therefore, the channels are not congested. Also, the channel utilization decreases from data channel 1 to data channel 3, in concordance with what has been explained in the previous paragraph. On the other hand, Figure 11a shows the number of data channels used (n) to transmit the data as the simulation time increases, while Figure 11b shows the probability that one or more channels are employed. It can be observed in both figures how, as the network size is increased, it becomes more congested, and therefore a greater number of data channels is needed to transmit the NAN applications.



(a) On-demand mode. Reactive routing information lifetime: 5.12 s.

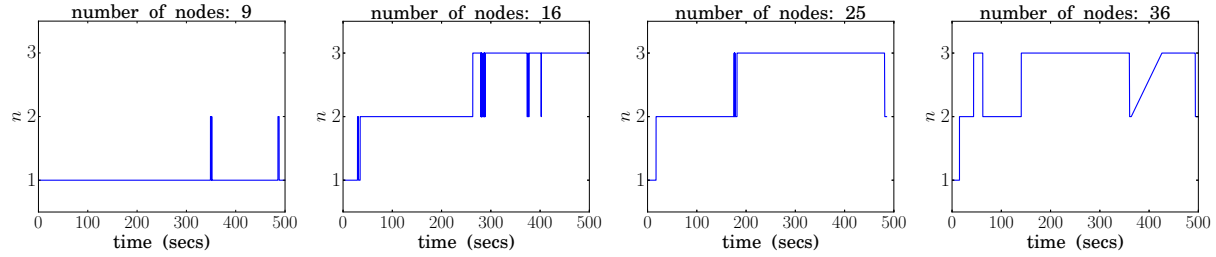


(b) On-demand mode. Reactive routing information lifetime: 0.512 s.

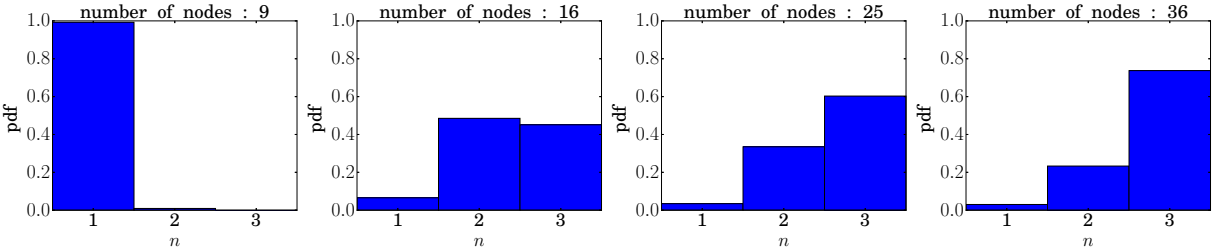


(c) Proactive mode. Proactive routing information lifetime: 5.12 s.

Figure 10: Channel utilization factor.



(a) channel occupancy (temporary evolution).

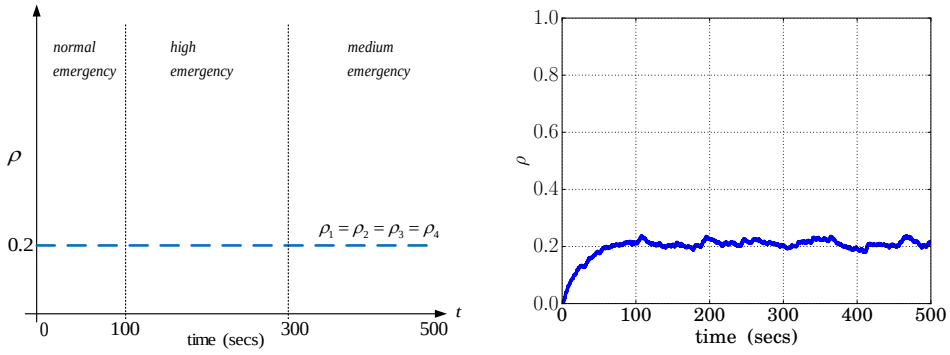


(b) channel occupancy (pdf).

Figure 11: Channel occupancy for the EA-HWMP. On-demand mode. Reactive routing information lifetime: 5.12 s.

4.2. Emergency scenario

In the present scenario, the channel allocation and traffic differentiation techniques, congestion control mechanism and the emergency system are implemented and evaluated together. For this purpose, some modifications were made to the previous scenario. First, NAN applications were configured to generate the same amount of data for all types of traffic (Figure 12). Second, four emergency sub-scenarios are considered (normal, medium, high and a combination of the previous three). The purpose it to evaluate how the congestion control functions are adapted to the different emergency situations. That is, to give a greater probability of transmission to the most important traffics, specially in emergency situations. These situations are set up by using broadcast messages. For the first three sub-scenarios, at the beginning of the simulation an emergency message is sent by a node to indicate the type of emergency situation throughout the network. On the other hand, in the last sub-scenario (combined) three packets are sent at different times (Figure 12a). At the beginning of the simulation (t=0) a normal emergency situation message is transmitted, after 100 seconds a medium emergency situation message is sent, and then after 300 seconds a message of medium emergency situation is sent. The results are evaluated with the same figures of merit (packet delivery ratio, throughput, transit time and channels occupation) and tools used in the previous scenario.



(a) target ρ.

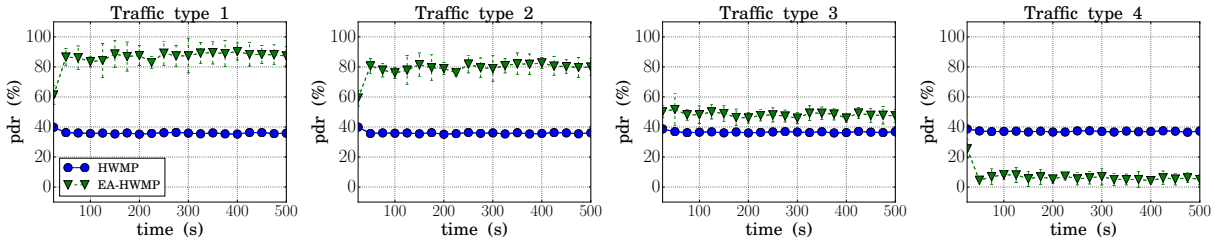
(b) measured ρ.

Figure 12: Traffic generation for the different NAN applications for the emergency scenarios.

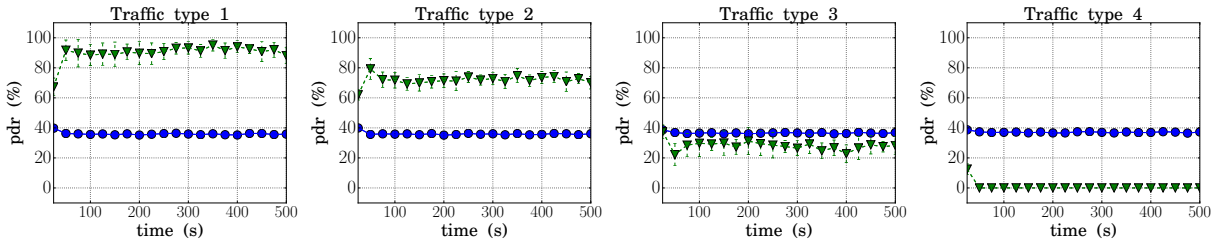
4.2.1. Packet delivery ratio and network throughput

In this subsection, the benefits obtained in terms of packet delivery ratio and throughput are presented in the same two ways as the previous scenario but with some differences. First, HWMP and EA-HWMP are compared taking into account the temporary evolution of the PDR and throughput. Second, the global average values are analyzed.

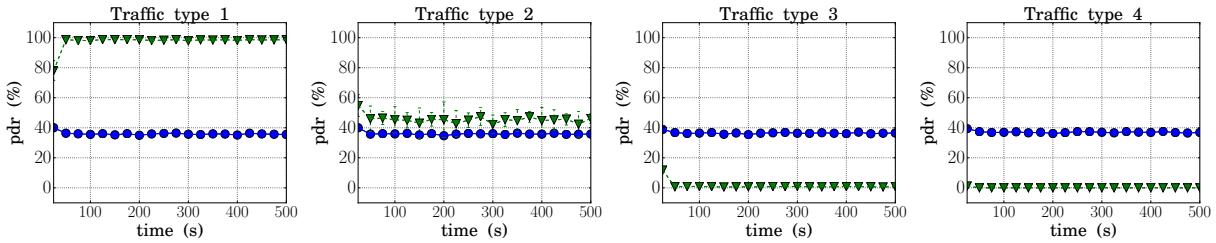
Figures 13 and 14 show the PDR and throughput evolution over time for the four emergency scenarios and the four traffic types. For the first three scenarios, the same results are highlighted. The PDR and throughput are increased for the higher priority traffic, and these values are increased even more when the emergency situation is high. On the other hand, in situations of high emergency, lower priority NAN applications are discarded, and therefore the PDR and throughput are reduced. In the combined case, as mentioned, the scenario goes from a normal emergency situation (0 to 100 s), to a medium (100 to 300 s) and ends in a high emergency situation (300 to 500 s). The changes of emergency situations can be clearly seen in Figures 13d and 14d. In a high emergency situation, the system adapts the congestion control functions in order to give a greater probability to NAN applications grouped as traffic type 1. This can be seen with the increase of PDR and throughput from 100 to 200 s. However, the price to pay is a fall of these parameters for the less priority traffic. In the last stage, the PDR and throughput increase when going from high to medium emergency situation.



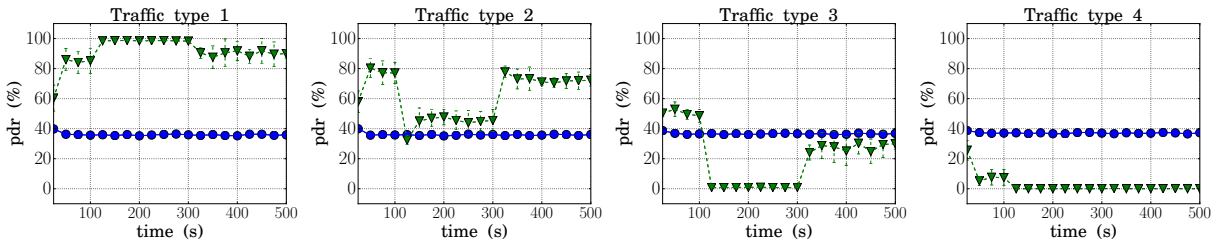
(a) Emergency situation: normal.



(b) Emergency situation: medium.

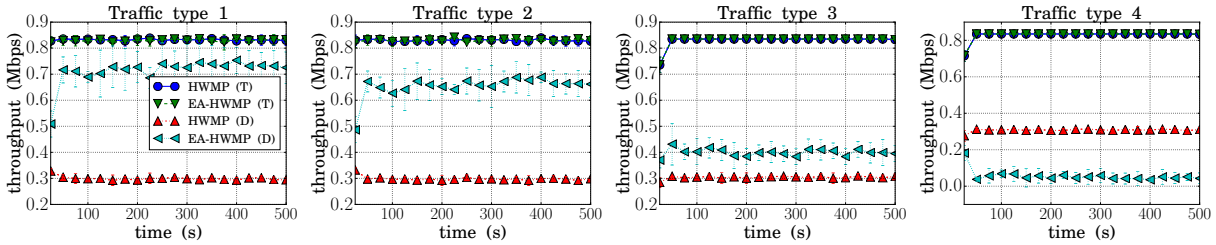


(c) Emergency situation: high.

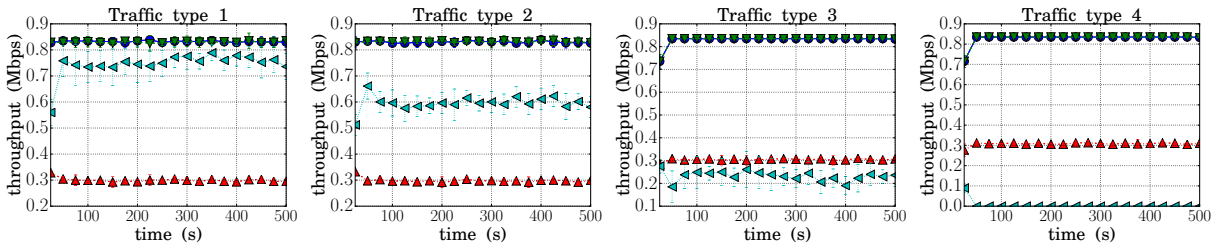


(d) Emergency situation: combined.

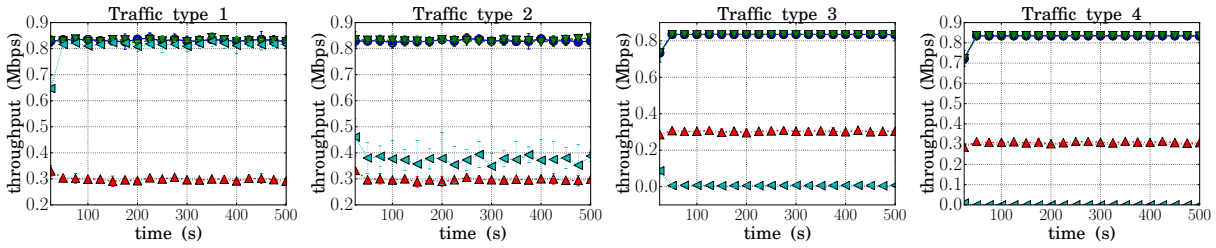
Figure 13: Packet delivery ratio evolution over the time for different emergency situations (network size: 25).



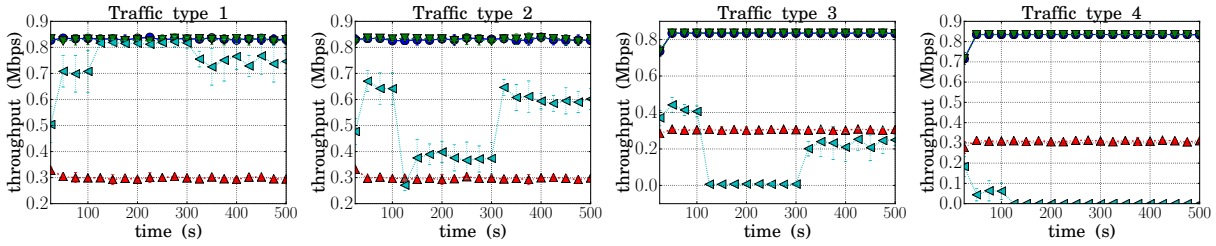
(a) Emergency situation: normal.



(b) Emergency situation: medium.



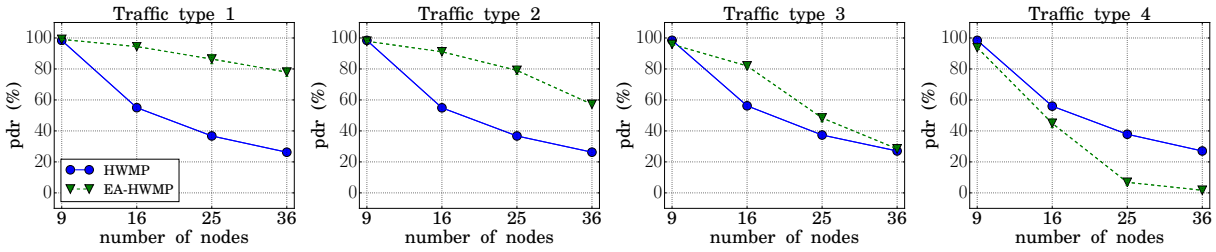
(c) Emergency situation: high.



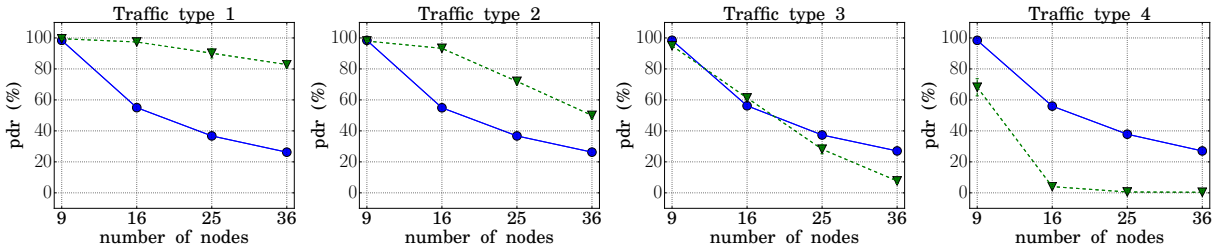
(d) Emergency situation: combined.

Figure 14: Network throughput evolution over the time (network size: 25).

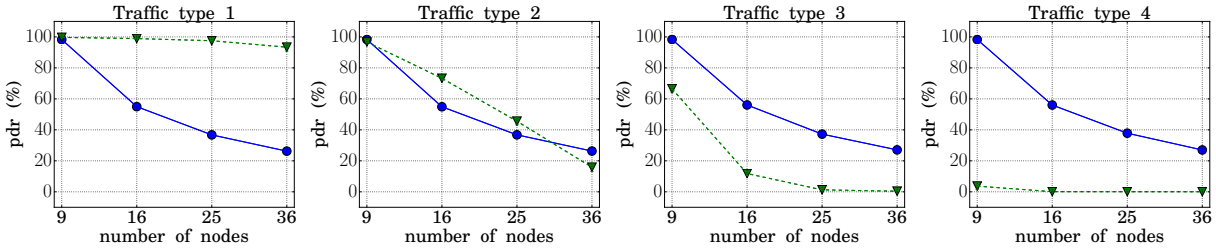
The PDR and throughput average values (together with the 95% confidence interval) are shown in Figures 15 and 16, for different network sizes. As the network size is increased, it becomes more congested and so the PDR decreases for all traffics (Figure 15). However, it is important to highlight some important aspects. On the one hand, this decrease is smaller with EA-HWMP for priority traffic types. In addition, emergency situations give a greater probability of transmission to the most important traffic. Therefore, the PDR is increased from the normal emergency situation to the high one for the traffic type 1. Meanwhile, for the less priority traffic types, the PDR is reduced by discarding packets of some NAN applications. On the other hand, Figure 16 complements the result obtained by the PDR parameter. That is, the network throughput is higher for traffic type 1, and it is even greater for the high emergency situation. For the less priority traffic types, the throughput decreases when the emergency situation changes from normal to high.



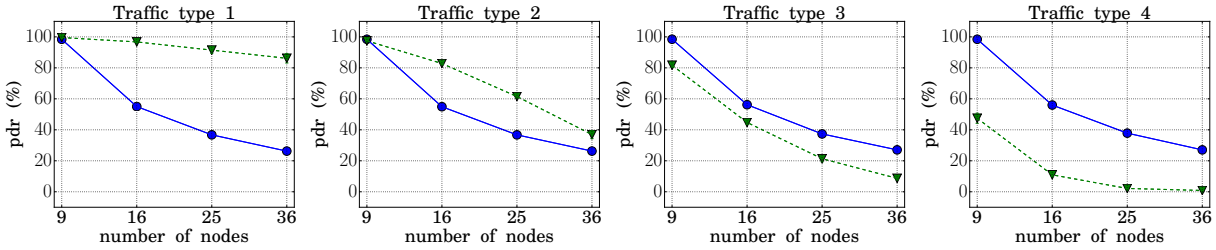
(a) Emergency situation: normal.



(b) Emergency situation: medium.

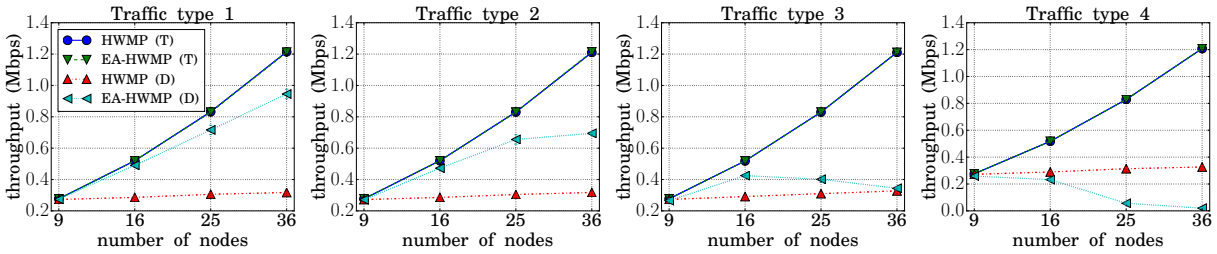


(c) Emergency situation: high.

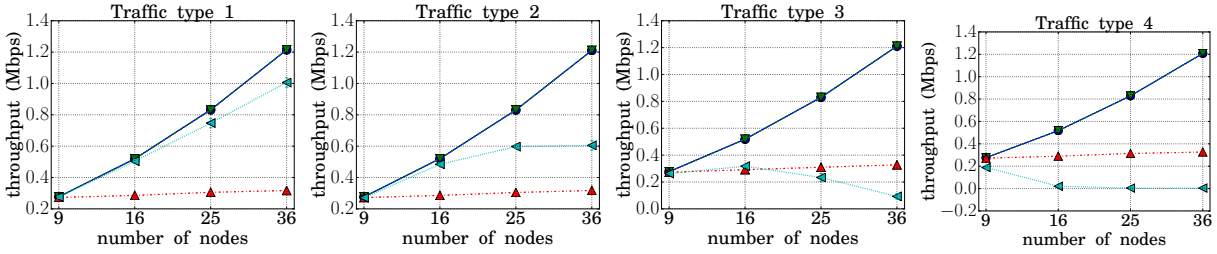


(d) Emergency situation: combined.

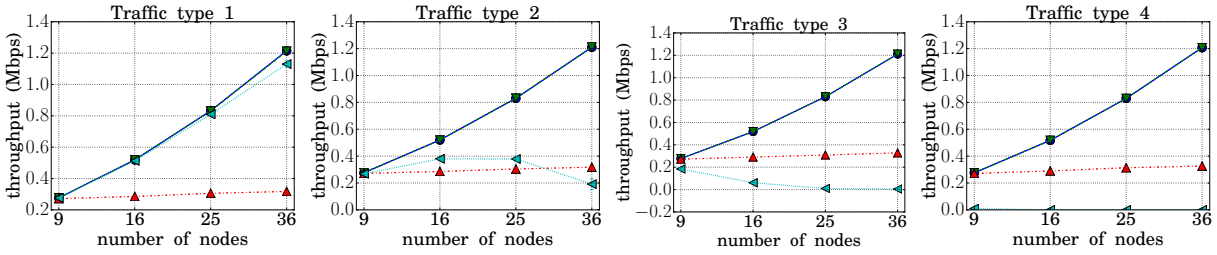
Figure 15: Packet delivery ratio for different emergency situations.



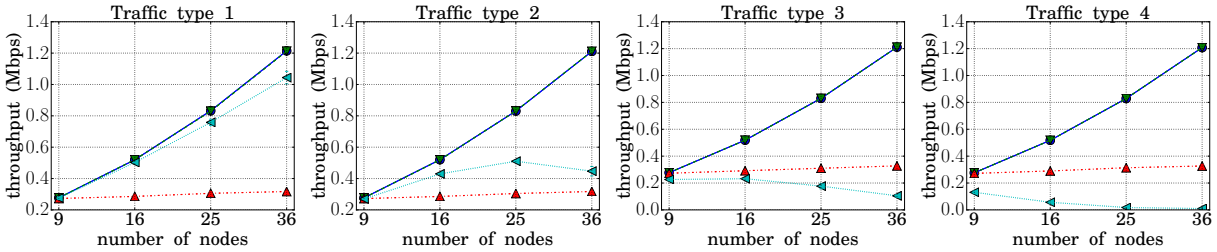
(a) Emergency situation: normal.



(b) Emergency situation: medium.



(c) Emergency situation: high.

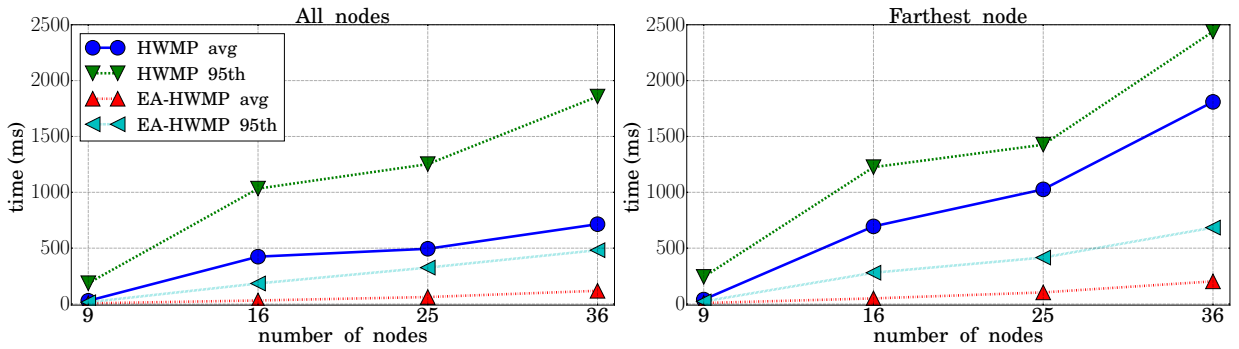


(d) Emergency situation: combined.

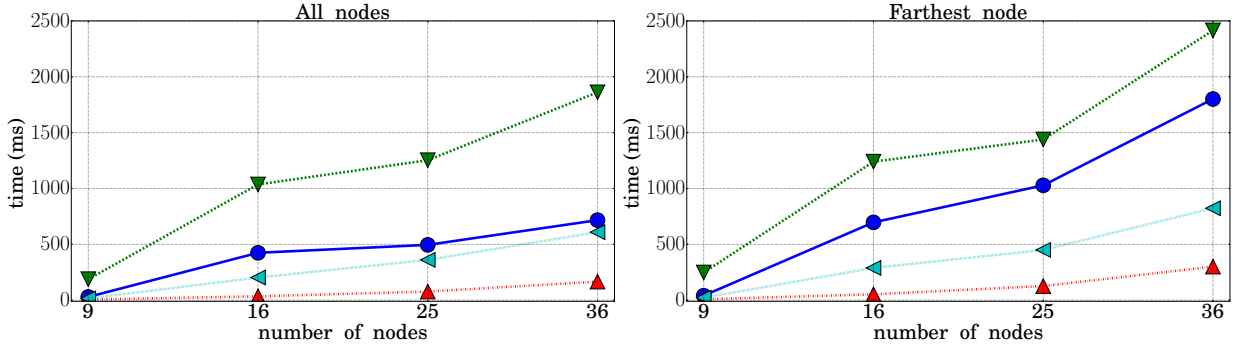
Figure 16: Network throughput for different emergency situations.

4.2.2. Network transit time

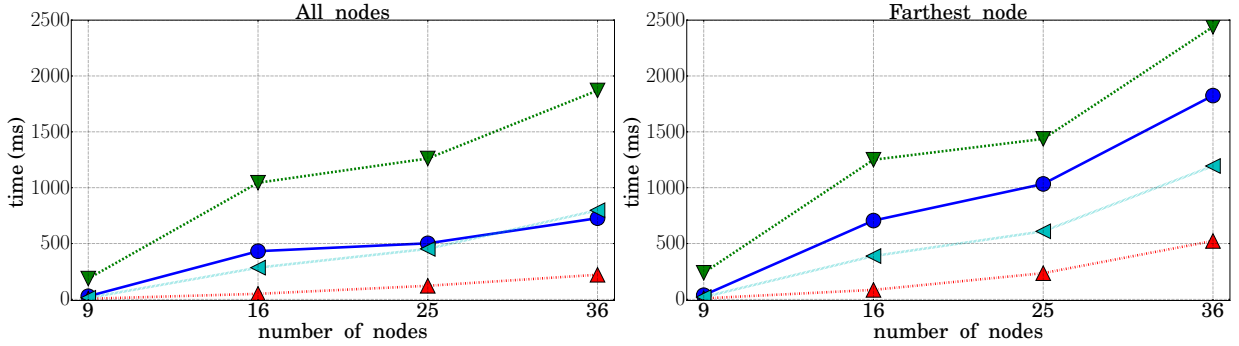
In the same way as the previous scenario, the analysis of the percentiles of the transit time, together with the average values are presented, both averaged for all the network nodes, and taking into account only the node farthest from the concentrator. Figure 17 shows the results for the combined scenario. As can be seen, these values are always lower (for all network sizes and for all types of traffic) when using the techniques proposed in this article. Similarly, a significant improvement is observed in the average and percentile values obtained in the farthest node case.



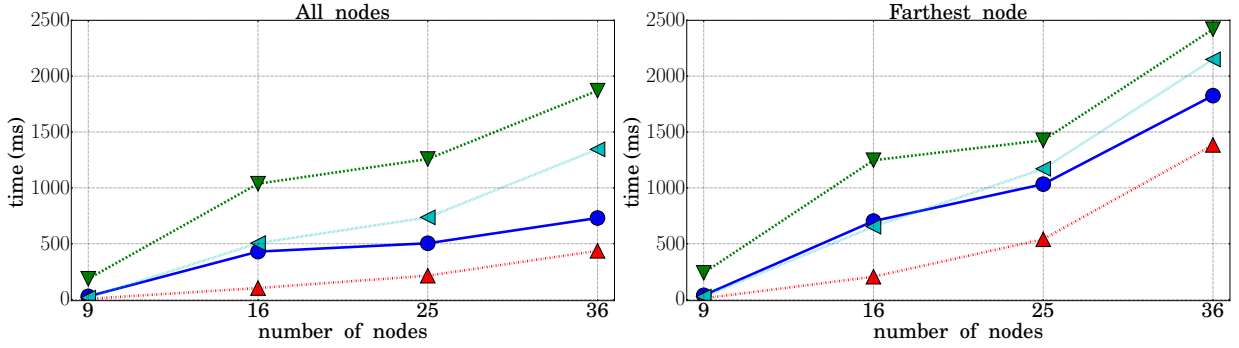
(a) Traffic type 1.



(b) Traffic type 2.



(c) Traffic type 3.

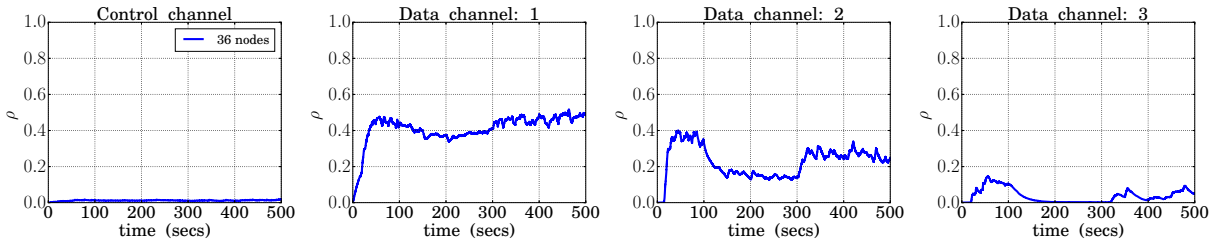


(d) Traffic type 4.

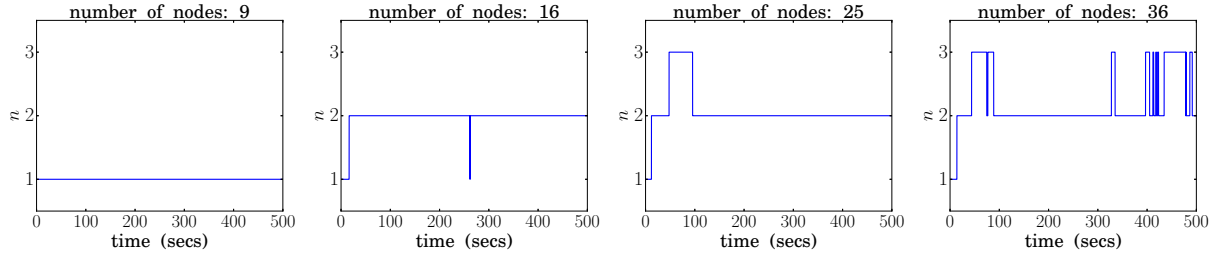
Figure 17: Network transit time (Emergency situation: combined).

4.2.3. Channel utilization factor

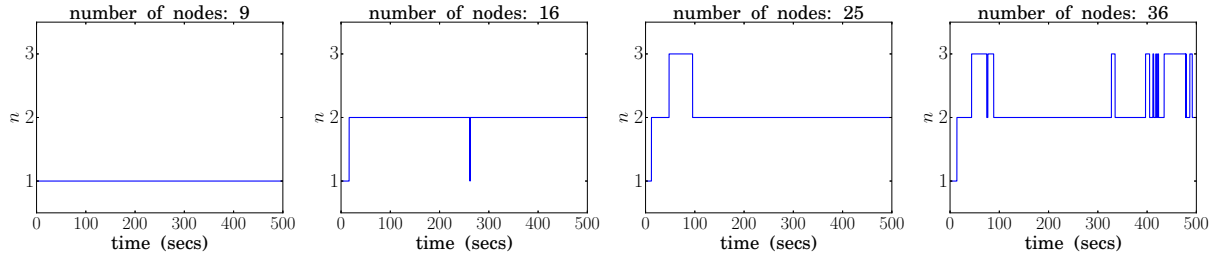
Figure 18a shows the channel utilization factor measurement for the EA-HMMP protocol, for the nearest smart meter node to the concentrator, and for the four available channels (one control channel and three data channels). As in the previous scenario, it can be seen how the control channel, dedicated to transmit only emergency and routing control messages, is never congested, since its ρ value is very low. Also, data channels are not congested, since the value of ρ never reaches high values (always below the ρ threshold). On the other hand, the channel utilization decrease from the data channel 1 to the data channel 3, and in particular, data channel 2 presents the fall of the value of ρ (100 to 300s) when the system is in a high emergency situation. Finally, Figures 18b and 18c show the results for the channel occupancy in terms of temporary evolution and probability. In the same way as the previous scenario, it can be seen how as the network size is increased, a greater number of channels are used to transmit the applications.



(a) ρ measured.



(b) channel occupancy (temporary evolution).



(c) channel occupancy (pdf).

Figure 18: Channel occupancy for the EA-HWMP (emergency situation: combined).

5. Conclusions

In this paper, we have evaluated the feasibility of implementing an emergency aware congestion control mechanism in the context of Smart Grid Neighborhood Area Networks. For this purpose, a Wireless Mesh Network is used as the network technology and smart meters as mesh STA devices. First, the proposed mechanisms allow identifying the different applications and grouping them into different types of traffic. Second, different congestion control functions have been configured for each traffic type. These functions are intended to give a higher transmission probability to NAN applications with higher priority in situations of network congestion. In addition, these functions are adapted depending on the emergency situation. That is, in a high emergency situation, the transmission probability is increased even more for priority traffic types by discarding applications with lower QoS requirements. Also, our

proposal works together with a channel allocation technique. This mechanism separates control and data traffic into separate channels. On the one hand, a dedicated control channel is responsible for transmitting routing and emergency messages. In particular, emergency messages must be transmitted to the whole network in the shortest time possible, and therefore a dedicated channel has been used to avoid unnecessary delays that may be caused by network load on the data channels. On the other hand, the rest of available channels are used to transmit the different NAN applications. The objective of our proposal is to use the least amount of data channels, while keeping the desired QoS for all traffic types. For this, one more channel will be used to transmit the data if and only if the current channel is busy ($\rho_{ch} > \rho_{th}$). Finally, if all the channels are busy, the packets are discarded.

In order to evaluate our proposal, two network scenarios have been evaluated (congestion control and emergency). Besides, the number of nodes present in the grid is increased (from 9 to 36 nodes), which gives rise to a greater contention in the access to the shared medium. First, the congestion control scenario is evaluated with three different network loads (normal, medium and high), and without using the emergency aware mechanism. For this scenario, the number of the data flows for traffic type 1 is increased during the medium network load, while the packet generation rate for the other traffic types are remained the same for all the simulation. From the obtained results, it can be seen that in situations of network congestion, our proposal mechanism overcomes the basic protocol in terms of packet delivery ratio, throughput and transit time for priority traffic types and for all network sizes. Second, with the emergency scenario, we have evaluated the network performance when the channel allocation and traffic differentiation techniques, congestion control mechanism and the emergency system are implemented together. In this scenario, NAN applications were configured to generate the same amount of data for all traffic types, and also four emergency sub-scenarios are considered (normal, medium, high and a combination of the previous three). These emergency situations were propagated through the whole network by using broadcast messages. It can be seen from the results that emergency aware mechanism benefits the traffic with higher QoS requirements in situations of high emergency. It can be noticed clearly in the combined emergency sub-scenario how the PDR and the delivered throughput are modified according to the emergency situation configured.

As future lines of work, our research to improve NANs performance will continue by adding dynamic adaptation of congestion control functions and detection and triggering of emergency situations through some indicators such as ρ_{ch}, frame losses or transit time. For this purpose, new extensions for the HWMP protocol will be proposed.

Acknowledgments

This work was supported by the Spanish Research Council under projects INRISCO (TEC2014-54335-C4-1-R) and MAGOS (TEC2017-84197-C4-3-R), and Juan Pablo Astudillo León is the recipient of a full scholarship from the Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), Ecuador.

References

[1] N. Shaukat, S. Ali, C. Mehmood, B. Khan, M. Jawad, U. Farid, Z. Ullah, S. Anwar, M. Majid, A survey on consumers empowerment, communication technologies, and renewable generation penetration within smart grid, Renewable and Sustainable Energy Reviews 81 (2018) 1453 – 1475. doi:https://doi.org/10.1016/j.rser.2017.05.208.
URL http://www.sciencedirect.com/science/article/pii/S1364032117308420

[2] W. Meng, R. Ma, H. Chen, Smart grid neighborhood area networks: a survey, IEEE Network 28 (1) (2014) 24–32. doi:10.1109/MNET.2014.6724103.

[3] A. Ikpehai, B. Adebisi, K. M. Rabie, Broadband plc for clustered advanced metering infrastructure (ami) architecture, Energies 9 (7). doi:10.3390/en9070569.
URL http://www.mdpi.com/1996-1073/9/7/569

[4] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G. P. Hancke, A Survey on Smart Grid Potential Applications and Communication Requirements, IEEE Transactions on Industrial Informatics 9 (1) (2013) 28–42. arXiv:arXiv:1011.1669v3, doi:10.1109/TII.2012.2218253.
URL http://ieeexplore.ieee.org/document/6298960/

[5] W. Liao, S. Salinas, M. Li, P. Li, K. A. Loparo, Cascading failure attacks in the power system: A stochastic game perspective, IEEE Internet of Things Journal 4 (6) (2017) 2247–2259. doi:10.1109/JIOT.2017.2761353.
URL http://ieeexplore.ieee.org/document/8063873/

[6] Y. Tsado, K. A. A. Gamage, D. Lund, B. Adebisi, Performance analysis of variable Smart Grid traffic over ad hoc Wireless Mesh Networks, in: 2016 International Conference on Smart Systems and Technologies (SST), IEEE, 2016, pp. 81–86. doi:10.1109/SST.2016.7765637.
URL http://ieeexplore.ieee.org/document/7765637/

[7] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), Internet Engineering Task Force (IETF) 4 (2003) 75. arXiv:arXiv:1011.1669v3, doi:10.1.1.11.620.
URL https://www.ietf.org/rfc/rfc3626.txt

[8] Ieee standard for information technology- telecommunications and information exchange between systems local and metropolitan area networks specific requirements part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, ieee std 802.11-2016 (revision of ieee std 802.11-2012), pp. 13534, IEEE Computer Society.

[9] Y. Tsado, K. Gamage, B. Adebisi, D. Lund, K. Rabie, A. Ikpehai, Improving the Reliability of Optimised Link State Routing in a Smart Grid Neighbour Area Network based Wireless Mesh Network Using Multiple Metrics, Energies 10 (12) (2017) 287. doi:10.3390/en10030287.
URL http://www.mdpi.com/1996-1073/10/3/287

[10] J.-S. Jung, K.-W. Lim, J.-B. Kim, Y.-B. Ko, Y. Kim, S.-Y. Lee, Improving IEEE 802.11s Wireless Mesh Networks for Reliable Routing in the Smart Grid Infrastructure, in: 2011 IEEE International Conference on Communications Workshops (ICC), IEEE, 2011, pp. 1–5. doi:10.1109/iccw.2011.5963578.
URL http://ieeexplore.ieee.org/document/5963578/

[11] J. Kim, D. Kim, K.-W. Lim, Y.-B. Ko, S.-Y. Lee, Improving the reliability of IEEE 802.11s based wireless mesh networks for smart grid systems, Journal of Communications and Networks 14 (6) (2012) 629–639. doi:10.1109/JCN.2012.00029.
URL http://ieeexplore.ieee.org/document/6412861/

[12] X. Deng, L. He, C. Zhu, M. Dong, K. Ota, L. Cai, QoS-Aware and Load-Balance Routing for IEEE 802.11s Based Neighborhood Area Network in Smart Grid, Wireless Personal Communications 89 (4) (2016) 1065–1088. doi:10.1007/s11277-016-3305-x.
URL http://link.springer.com/10.1007/s11277-016-3305-x

[13] X. Deng, Q. Peng, L. He, T. He, Interference-aware qos routing for neighbourhood area network in smart grid, IET Communications 11 (5) (2017) 756–764. doi:10.1049/iet-com.2016.0860.
URL https://ieeexplore.ieee.org/document/7901970

[14] X. Deng, T. He, L. He, J. Gui, Q. Peng, Performance analysis for ieee 802.11s wireless mesh network in smart grid, Wireless Personal Communications 96 (1) (2017) 1537–1555. doi:10.1007/s11277-017-4255-7.
URL https://doi.org/10.1007/s11277-017-4255-7

[15] H. Gharavi, B. Hu, Multigate Communication Network for Smart Grid, Proceedings of the IEEE 99 (6) (2011) 1028–1045. doi:10.1109/JPROC.2011.2123851.
URL http://ieeexplore.ieee.org/document/5768102/

[16] X. Deng, L. He, X. Li, Q. Liu, L. Cai, Z. Chen, A reliable QoS-aware routing scheme for neighbor area network in smart grid, Peer-to-Peer Networking and Applications 9 (4) (2016) 616–627. doi:10.1007/s12083-015-0331-5.
URL http://link.springer.com/10.1007/s12083-015-0331-5

[17] K. A. Khaliq, A. Qayyum, J. Pannek, Performance Analysis of Proposed Congestion Avoiding Protocol for IEEE 802.11s, International Journal of Advanced Computer Science and Applications 8 (2) (2017) 356–369. doi:10.14569/IJACSA.2017.080246.
URL http://dx.doi.org/10.14569/IJACSA.2017.080246

[18] J. G. Jetcheva, S. Kailas, S. Kanodia, M. Natarajan, Multi-channel assignment method for multi-radio multi-hop wireless mesh networks, uS Patent 8,824,380 (Sep. 2 2014).

[19] S. Ghannay, S. M. Gammar, F. Filali, F. Kamoun, Multi-radio multi-channel routing metrics in ieee 802.11s based wireless mesh networks, annals of telecommunications - annales des télécommunications 67 (5) (2012) 215–226. doi:10.1007/s12243-011-0253-z.
URL https://doi.org/10.1007/s12243-011-0253-z

[20] A. A. Al Islam, M. J. Islam, N. Nurain, V. Raghunathan, Channel assignment techniques for multi-radio wireless mesh networks: A survey, IEEE Communications Surveys & Tutorials 18 (2) (2016) 988–1017. doi:10.1109/COMST.2015.2510164.
URL https://ieeexplore.ieee.org/document/7360096

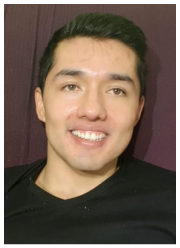
[21] M. Doraghinejad, H. Nezamabadi-pour, A. Mahani, Channel assignment in multi-radio wireless mesh networks using an improved gravitational search algorithm, Journal of Network and Computer Applications 38 (2014) 163 – 171. doi:https://doi.org/10.1016/j.jnca.2013.04.007.
URL http://www.sciencedirect.com/science/article/pii/S1084804513001100

[22] Y. Wu, F. Hu, S. Kumar, J. D. Matyjas, Q. Sun, Y. Zhu, Apprenticeship learning based spectrum decision in multi-channel wireless mesh networks with multi-beam antennas, IEEE Transactions on Mobile Computing 16 (2) (2017) 314–325. doi:10.1109/TMC.2016.2548461.
URL http://ieeexplore.ieee.org/document/7444189

[23] J. P. Astudillo León, L. J. de la Cruz Llopis, Multi channel allocation and congestion control for smart grid neighborhood area networks, in: Proceedings of the 15th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, PE-WASUN'18, ACM, New York, NY, USA, 2018, pp. 1–8. doi:10.1145/3243046.3243050.
URL http://doi.acm.org.recursos.biblioteca.upc.edu/10.1145/3243046.3243050

[24] J. Kim, D. Kim, K.-w. Lim, Y.-b. Ko, S.-y. Lee, Improving the reliability of IEEE 802.11s based wireless mesh networks for smart grid systems, Journal of Communications and Networks 14 (6) (2012) 629–639. doi:10.1109/JCN.2012.00029.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6412861

[25] ns 3 Network Simulator. (Available: http://www.nsnam.org/).



Juan Pablo Astudillo León is a Ph.D candidate in the SISCOM (Smart Services for Information Systems and Communication Networks) research group at the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain. He received the Electronics Engineering degree in 2012 from the Universidad Politécnica Salesiana, Cuenca, Ecuador, and the Master's degree

in Telecommunications Engineering and the Specialist degree in Telecommunications Technologies from the Universidad de Buenos Aires in 2014 and 2015 respectively. He was also an assistant professor at the Universidad Politéctnica Salesiana until 2016. His research includes Wireless Mesh Networks, Smart Grids and Traffic Engineering.

Luis J. de la Cruz Llopis received the telecommunication engineering degree in 1994 and the Ph.D. in telecommunications engineering in 1999, both from the Universitat Politécnica de Catalunya (UPC), Barcelona, Spain. He is currently an Associate Professor at the Department of Network Engineering of the UPC. His current research interests include wireless networks and IoT smart services.