Design and Implementation of a Cooperative Protocol for Extending Coverage in Wireless Mesh Networks

Andres Cabrera-Lozoya, Fernando Cerdan, Sergio Lujan, Diego Garcia-Sanchez
Department of Information and Communications Technologies
Universidad Politécnica de Cartagena, UPCT
Plaza del Hospital, 1, 30202, Cartagena, SPAIN
{andres.cabrera, fernando.cerdan, sergio.lujan, diego.gsanchez}@upct.es

***Abstract*—Wireless mesh networks (WMNs) have attracted great attention in the last few years because of their advantages over traditional wireless networks. WMNs can be seen as a mixture of ad hoc and infrastructure networks, with all the underlying benefits of such hybrid architecture. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops through intermediate nodes which not only boost the signal, but cooperatively act extending the network coverage and even forwarding decisions based on their knowledge about the network itself. This paper presents the main design and implementation aspects of a cooperative protocol that allows the coverage extension in these WMNs. It also provides a power saving mechanism for nodes which mainly operate as gateways by simply relaying data from or to neighbouring nodes. Simulation results show that the introduction of the protocol drastically increases the volume of carried traffic on the network due to its coverage extension capabilities. They also show that the power saving mechanism works properly, thus introducing key configuration parameters in the design of WMNs.**

Keywords - wireless mesh network; coverage extension; power saving mechanism; performance evaluation

I. INTRODUCTION

Recent economic emergence of wireless communication and portable computing devices together with the advances in communication infrastructures have produced the rapid growth of today mobile wireless networks. This has led to an exponential growth of cellular networks based on a combination of wired and wireless technologies.

However, the interest of scientific and industrial communities in the telecommunications field has recently changed towards the development of mobile networks with no fixed infrastructure. In this sense, ad hoc networks have become the cutting-edge technology in wireless communications. Indeed, these networks constitute the first step towards providing cost effective and dynamic high-bandwidth solutions over specific coverage areas. They allow the interconnection of the network nodes directly using wireless transceivers (usually through *multihop* paths) without the existence of a fixed infrastructure. This is a very distinctive feature of ad hoc networks compared to traditional wireless networks like cellular or wireless local area networks (WLANs), where nodes communicate with each other only through fixed stations.

On the other hand, WMNs have attracted great attention in the last few years since they can be seen as a mixture of ad hoc and infrastructure networks. Basically, they are infrastructure networks which allow the connection of devices out of the range of the access points (APs) through a direct connection with any node or device that is directly or indirectly within the coverage range of one of those APs. However, it seems that nowadays one of the main bottlenecks of this technology deals with the power consumption of the nodes and the communication's energetic efficiency. In this sense, every effort to develop energy-efficient protocols should be considered as an important contribution to the whole technology development.

This paper is structured as follows: Section II presents some related work in the area, enumerating several interesting experiences and investigations conducted in the last years in this field. In this regard, they will be classified depending on their scope and main aims, giving in turn a brief overview of the state of the art in this area of research.

Next, Section III presents the proposed application scenario for the protocol itself. Assumptions referring to the hardware involved and its mode of operation will be presented here. Advantages of using an ad hoc / infrastructure hybrid network will also be discussed.

Section IV deals with the formal specification of the protocol, where the key aspects of its operation will be explained from a qualitative point of view.

Section V presents the simulation's scenario and shows the results obtained during this process. In this section, the highlights of the protocol and its main advantages will be discussed from a quantitative point of view.

Finally, conclusions and future work are presented.

II. RELATED WORK

In the last few years, mesh networks have become an area of ongoing research due to its nature and potential applications. Nowadays, it is extremely easy to find mesh applications in many different scenarios [1, 2].

Thus, although mesh technology depends on other underlying technologies for the establishment of the network backhaul, these networks can indeed be deployed over almost any existing wireless technology, e.g. WiFi (for LAN environments), WiMAX (for MAN environments), etc. and once done, even coexist [3]. That said, it certainly seems that

 ISBN: 978-1-61208-147-2

wireless mesh networks are going to be ubiquitous and a line of intense research in a very near future.

Moreover, although the concept of hybrid cellular / ad hoc network is not new [4, 5], it represents an interesting line of action at present due to its nice features.

Indeed, we are steadily witnessing progress in routing techniques and protocols based on channel allocation and transfer rates in wireless mesh networks such as [6, 7], amongst many others. We are also witnessing that the implementation of proactive, reactive and hybrid protocols for optimizing these network traffics is also attracting great attention, like in [8], but despite of all, there are several aspects dealing with the optimization of the available resources in terms of power saving and energy consumption in these WMNs which currently pose a challenge to the researchers.

Thus, although even the most complex problems of mesh topology such as those related to the conduct of the nodes [9] or the network security itself [10] are progressively being addressed, energy consumption issues constitute a bottleneck for this technology at the moment.

The work presented in this paper attempts to shed some light on the development of coverage extension mesh protocols with power saving features which, in fact, is an area of intense research at the moment.

III. THE PROPOSED SCENARIO

This section describes the network which has been used to extensively test the protocol. In this sense, every hardware aspect relevant to the protocol implementation will be explained below.

A. Initial scenario

In this initial stage we will define the *server* as a single computer or access point that will continuously monitor all the network performance. This topology clearly corresponds to a centrally managed network scheme. This single device will count on a wireless interface and will be responsible for creating and maintaining a point to multipoint network in infrastructure mode to connect the various nodes in the network. All traffic generated by the nodes will always be directed to this server machine, making it possible to count and therefore process all data transactions between every node in the network.

Also, we will define the *nodes* or *mobile terminals* as portable devices powered, in any case, by batteries. Therefore, they will feature low processing power and limited energy resources. Each node will have two pre-configured wireless interfaces, using one for direct connection to the server (in infrastructure mode) and the other for direct communication with the rest of nodes through a multi-node topology, also called ad hoc network.

By default, all nodes will try to communicate through the network in infrastructure mode, using the ad hoc network only for communication with terminals outside the coverage area of the network server (see Fig. 1 below).

In this specific scenario, *covered nodes* (nodes within the coverage area of the server) will use the network in infrastructure mode to send / receive data, and *virtually-covered nodes* (nodes within the coverage range of another node which in turn has direct or indirect access *(through another node)* to the server) will use their ad hoc interface to communicate with their accessible nodes in each case.

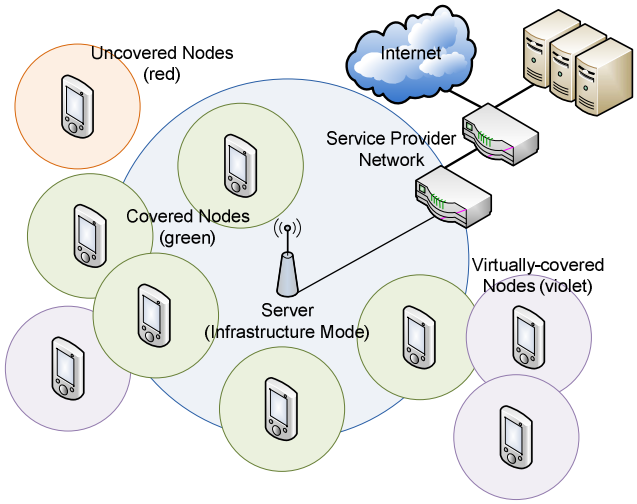

Figure 1. Schema of the application scenario.

Obviously, if a covered node had to communicate with a virtually-covered one, it would use its ad hoc interface since the virtually-covered node is not directly connected to the server and thus not accessible through the former's infrastructure mode interface.

Now, if we see Fig. 1 again, we can make a nice graphical analogy with *Set Theory* to give an idea of the extended coverage of the network using this protocol. Thus, if we considered each circular coverage range of Fig. 1 as a *set*, we could say that the network coverage corresponds to the size of the *union set* of them all (excepting, of course, the range of the uncovered nodes).

Finally, for this scenario to be implemented correctly, it will be assumed that all nodes will be motivated to act selflessly [9], so users are deemed to cooperate with the proper working of the protocol.

B. Advantages of a mixed network (ad hoc / infrastructure)

The main reason for testing the protocol over a mixed network is that infrastructure and ad hoc networks are complementary.

Ad hoc networks are almost always exclusively composed of mobile devices while infrastructure networks have at least one device which is not battery-powered. This simple fact makes the nature and operation of both types of networks very different, each one with its own characteristics. With this idea in mind, we can emphasize once again that the fact of using a mixed architecture brings several advantages:

On the one hand, the base station (in infrastructure networks) is usually powered from the mains. This fact allows that the server itself has a greater processing capacity, very powerful wireless interfaces (for signal transmission)

 ISBN: 978-1-61208-147-2

and increased sensitivity at reception. In addition, infrastructure mode networks avoid the massive transmissions of data that usually take place in multihopping networks, which can even saturate them when various peripheral nodes generate a large amount of traffic. This advantage comes out from having a really extensive coverage area provided by the base station. In such a situation, connections are made directly to the server, thus obtaining a satisfactory communication between nodes with only two hops in the majority of generated traffic (with the server acting as the only gateway).

On the other hand, the integration of an ad hoc network with the previous infrastructure network can provide several interesting advantages too. For example, multihop functionality provided by ad hoc networks can be used to increase the operating range of a conventional infrastructure network when it is not possible to make a direct connection to the base station through adjacent nodes, i.e., instead of requiring a direct connection between the nodes and the base station, it is possible to reach the server through different paths using multihop compatible wireless devices. In this way, we get to cover "*black spots*" which would be inaccessible in a common infrastructure mode network.

IV. PROTOCOL BASELINE

After having highlighted the advantages of using a mixed network, we will proceed to define the main features of the protocol from a formal point of view.

A. Protocol specification

When a mobile terminal generates a message to any other node of the network there are two possibilities to send data:

- If the source node is within the coverage range of the server, the mobile terminal will send the message directly to the server in infrastructure mode, with the subsequent receipt confirmation by the latter.
- However, if the mobile terminal has no direct connection to the server, it will broadcast the message through its ad hoc interface.

Any message generated and sent by a mobile terminal will always reach the server: when a node receives any message from any other node, it will act as a gateway in any case, so it will not parse the data. Then, it will simply broadcast the message to make it reach the server. This fact has several relevant consequences: on the one hand, we can guarantee that all data messages will be properly quantified and monitored by the server since they reach it. We can also assure that nodes will not incur any overhead because of this ad hoc operation: every data transmission through this network will be broadcasted without any processing since the server is the only device capable of delivering data to nodes. On the other hand, we find that broadcasting will cause nodes to use a greater amount of resources than nodes which might analyze and accept the message as their own, preventing its spread towards the server.

There may be a multitude of mobile terminals acting as gateways between the server and the source and destination nodes, not only one.

When the server has a message to some node, the former will broadcast a test message to see if the desired node is within its coverage area (in both networks, if necessary):

- If so, it will selectively send the message to the recipient node, the latter replying with a receipt confirmation message.
- On the contrary, if the destination node is not within the coverage area, the server will search the recipient using the ad hoc network created by the nodes through multihop technique. There are two possibilities:
  - If the recipient is located, the server will selectively send data using multihop mechanism.
  - If the recipient is not located, the server will store data for a later retry.

Two approaches can be taken to send messages when the server needs to use the multihop network to reach nodes that are inaccessible through direct connection:

- When locating the mobile terminal, its routing path could be refreshed and stored inside the data message as it goes through the network towards the server. Then, the server could send the data message using that very route. This option allows further optimization of energy resources, but communications turn unstable because, e.g., if any of the gateway nodes used to route the message moves significantly, the transaction will be unsuccessful. This situation would cause the delivery mechanism of the protocol to perform all the steps above to try to transmit the message again. This is a common problem in networks with high mobility, e.g., when mobile terminals are inside vehicles.
- Another option consists of ignoring the route path to the recipient node when locating the mobile terminal. In this case, the reply message will only indicate the presence or absence of connectivity with the destination node. This *broadcasting option* results in a waste of energy by the nodes because the message delivery mechanism will affect a larger number of devices. However, we can ensure with a very high probability that recipient nodes will receive the messages, regardless of the type of network we are working with, since it is a more flexible protocol to network changes (*due to its broadcasting nature*). The cooperative protocol presented in this paper uses this type of location because *in this case* the reliability takes precedence over energy efficiency. Furthermore, in such mesh network environments reliability, self-reconfiguration and self-healing features must be predominant.

Moreover, the protocol includes a power saving mechanism to limit the energy consumption of the nodes which consistently act as gateways relaying messages from other nodes to / from the server (indirect messages) due to its possible location near the border of the coverage area of the fixed network. This mechanism leaves them in idle state during a time interval which is proportional to a *tiredness index* parameter (described in Section V below), that consists of a counter which increases each time the node relays an indirect message.

 ISBN: 978-1-61208-147-2

The interaction between the server and the destination node in each case will be independent of the emission mechanism used by the source node.

Fig. 2 below presents the protocol's high-level flowchart.

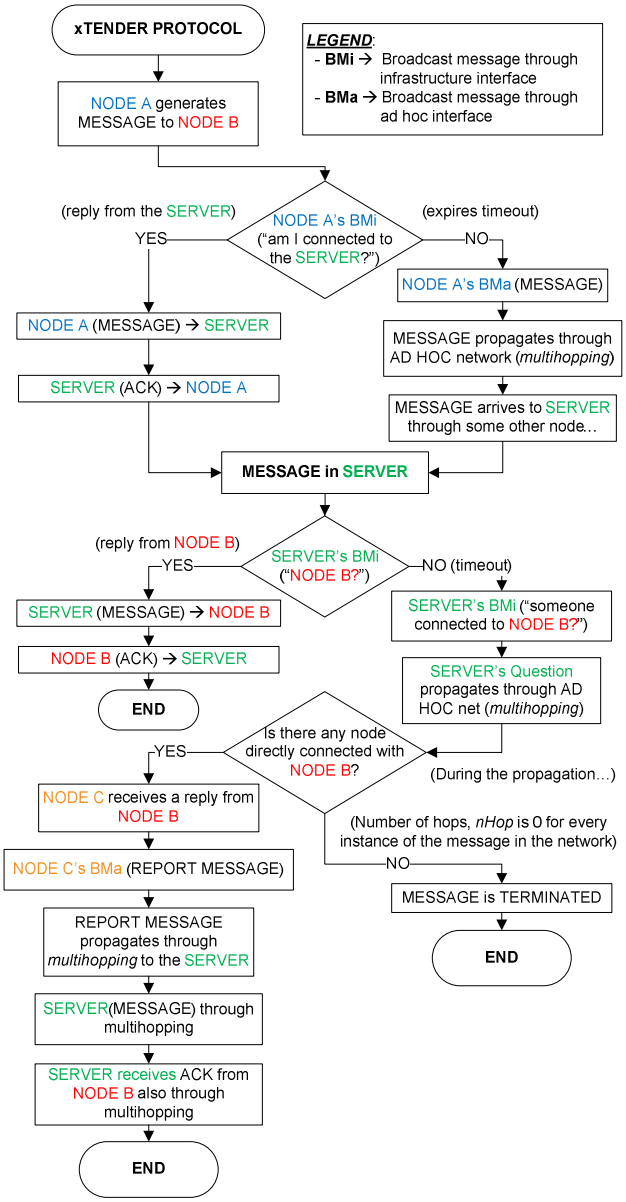

Figure 2. Protocol's high-level flowchart.

Finally, two mechanisms are used to prevent the network collapse:

- Each message will carry a hop counter which will limit the number of hops that a given message can perform.
- Each message will carry a unique identifier (*ID*) that will prevent the same message to be relayed more than once by any mobile terminal, thus avoiding infinite loops.

B. *Message definitions*

After having described the protocol behaviour, we now proceed to define the various messages to be used along with their features.

We could initially make a clear division towards their classification: on the one hand, we can find those messages that are transmitted directly between any node and the server. They will be called *direct messages*. On the other hand, we find those messages that are propagated through the network using multihopping techniques, for communication between terminals. They will be then called *indirect messages*. At this point, it is obvious that every time a terminal receives one of these messages, it will relay it using broadcasting except when the node itself is the destination terminal.

There are different types of messages within each family, and we can differentiate them through the various functions they perform, namely:

- Data transmission
- Receipt confirmation
- Node search

Direct messages (DM) can be sent by the server and the nodes. They count, at best, on the next fields: type of message (*ToM*), source address (*Src*), destination address (*Dst*), unique identifier (*ID*), data length (*Len*) and the data itself (*Data*). Table I below presents each message subtype along with it specific fields:

TABLE I. DIRECT MESSAGES FIELDS

Message subtype	*ToM*	*Src*	*Dst*	*ID*	*Len*	*Data*
Data Transmission	*	*	*	*	*	*
Receipt Confirmation	*	*	*	*		
Node search	*		*			

Indirect messages (IM) are only used for communication between terminals. IMs will only be sent by the server, through multihopping techniques. Thus, if the server receives one of these messages, it will delete it immediately. The fields present in IMs are the same as those of DMs, plus one: the number of hops (*nHop*), indicating in each case the maximum number of hops remaining for a message before it is discarded by the nodes, as a saturation control action. In this way, this mechanism is very similar to the well-known TTL (*Time To Live*) field to be found on many communications systems an protocols. Table II below presents each IM subtype along with it specific fields:

TABLE II. INDIRECT MESSAGES FIELDS

Message subtype	*ToM*	*Src*	*Dst*	*ID*	*Len*	*Data*	*nHop*
Data Transmission	*	*	*	*	*	*	*
Receipt Confirmation	*	*	*	*			*
Node search	*		*				*

 ISBN: 978-1-61208-147-2

In such a scenario, null signalling overhead is always guaranteed since nodes communicate with each other through a flooding mechanism, as explained above in Section IV.A, i.e., using broadcasted messages. Thus, datagrams (see Fig.3 below) do not need extra fields for nodes to know the routing path in each case (which would cause a signalling overhead, affecting the whole system's performance) since they do not even need to process any special headers to transmit or receive messages within the ad hoc network: they simply broadcast every message just as it arrives.

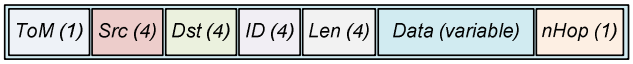

Figure 3. Detailed datagram structure (numbers in parentheses represent the lenght in bytes of each field).

V. PERFORMANCE EVALUATION

The protocol was developed, implemented and validated using the Specification and Description Language (SDL) and the SDL Tools branch (including SDL Simulator and SDL Validator). The proposed simulation scenario is described in Section III above.

A. Simulation Parameters

Some representative environment variables were externally declared from the outset in order to analyze the protocol behaviour and its efficiency. They were used to launch parametric simulations in which the variation of one or more of them made possible to obtain interesting simulation results. Below are presented each of the variables of the simulation environment along with its meaning and function:

- *nNodes*. It indicates the number of nodes present in a given simulation.
- *nConnec*. It sets the maximum number of connections between nodes, and therefore, in the boundary case, the maximum number of nodes that would be within the coverage area of every single node.
- *PG*. It represents the probability of a node to generate a message to another at a given point in time.
- *PC*. It represents the probability of a direct connection between the nodes and the server.
- *maxHop*. It defines the maximum number of hops that a message can perform when using multihopping technique.
- *indTired*. It indicates the increment of the tiredness rate of each node each time an indirect message is relayed.
- *Sleep*. It indicates how long a node will remain inactive / idle due to its *tiredness*.

(These two last variables are related to the power saving mechanism implemented in the protocol for the nodes).

B. Simulation Results

All the results shown in this section arise from the execution of a number of simulations with the same parameters, so that every result is consistent with the average of those simulations in each case.

We performed the following simulations:

- *Traffic Evolution with a variable PG parameter:*

Table III below shows a specific simulation scenario to study the network traffic evolution when the probability of generating messages by nodes, *PG*, varies from 0 to 1.

TABLE III. PARAMETER VALUES FOR SIMULATION 1

Parameter	*Value*	*Parameter*	*Value*
nNodes	15	*nConnec*	3
PC	0.3	*maxHop*	4
PG	Variable	*indTired*	Disabled

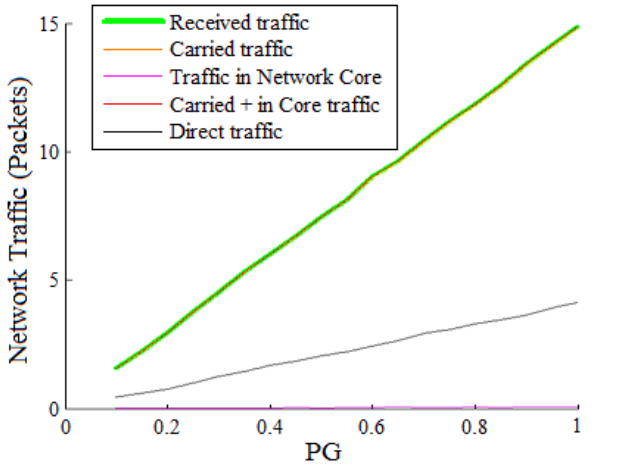

Figure 4. Network traffic evolution based on PG parameter

As can be seen in Fig. 4, obviously all types of traffic increase linearly with traffic generation. Furthermore, in this case all generated traffic is successfully carried since it has direct or indirect access to all nodes. However, the only traffic that could have been carried without the addition of the coverage extension protocol corresponds to the black line (direct traffic) on the figure. In this sense, it is very noteworthy that the addition of the protocol with this specific simulation resulted in a constant increment of around 350% of carried traffic volume coming to a maximum of 383% for PG = 0.2, as can be seen in Fig. 5 below.

 ISBN: 978-1-61208-147-2

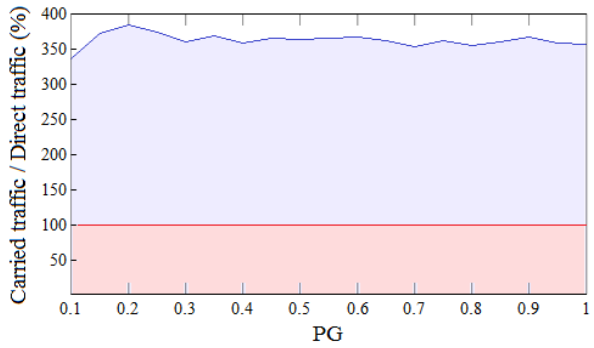

Figure 5. Increment of carried traffic volume when using the protocol compared to a normal situation (without the protocol) (%)

- *Traffic Evolution with a variable nConnec parameter:*

In this case, the simulation parameters shown in Table IV are focused on the study of the network traffic evolution when the maximum number of connections between nodes, *nConnec*, varies from 0 to 10.

TABLE IV. PARAMETER VALUES FOR SIMULATION 2

Parameter	*Value*	*Parameter*	*Value*
nNodes	15	*nConnec*	Variable
PC	0.125, 0.25	*maxHop*	10
PG	0.5	*indTired*	Disabled

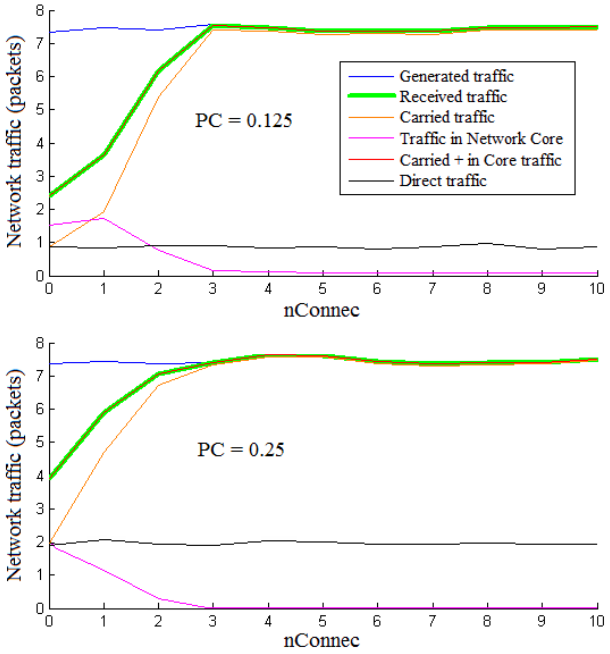

Figure 6. Network traffic evolution based on nConnec parameter with PC = 0.125 and 0.25, respectively

Fig. 6 shows the traffic evolution based on *nConnec* parameter. This simulation aimed to quantitatively analyze the effect of increasing the number of connections between nodes. Conclusions are simple but very meaningful: almost all of generated traffic is carried with an average of 3 connections between nodes although there is a low connectivity to the server in all these simulations (20 and 40% respectively).

- *Traffic Evolution with a variable indTired parameter:*

This third simulation was carried out to test the usefulness and efficiency of the power saving mechanism developed for the protocol. Table V below shows the list of parameters used in this simulation.

TABLE V. PARAMETER VALUES FOR SIMULATION 3

Parameter	*Value*	*Parameter*	*Value*
nNodes	15	*nConnec*	3
PC	0.4	*maxHop*	3
PG	0.8	*indTired*	Variable

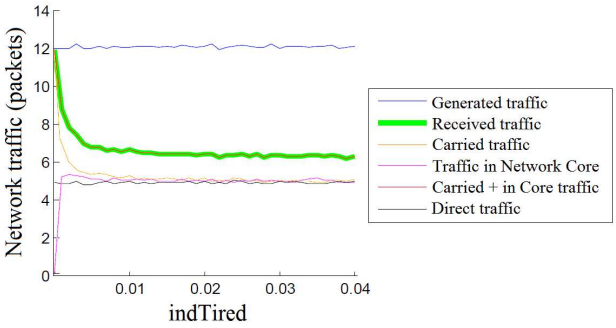

Figure 7. Network traffic evolution based on indTired parameter

Fig. 7 shows the effect of the power saving mechanism implemented for the protocol in the network traffic evolution. Here, as the *tiredness rate* of nodes grows, so does loss rate, slowing down from 0.01 for this specific tiredness index. As already discussed earlier in this paper, losses are due to the existence of nodes that have not direct connectivity to the server. Then, when they transmit data and relay nodes near them are idle, traffic is lost.

From these simulations, we could say that a value between 0 and 0.01 for the tiredness index parameter would be acceptable in terms of traffic losses. In this sense, the selection of a greater or lesser value is a pure design decision depending on every single network deployment and its requirements. Therefore, when designing a network using this cooperative protocol, *indTired* parameter should be carefully chosen to reach a compromise between network losses and energy saving in nodes.

 ISBN: 978-1-61208-147-2

VI. CONCLUSION

In this paper we have presented the main design and implementation aspects of a cooperative protocol that allows the coverage extension in wireless mesh networks. This protocol also includes power saving features for terminals which mainly operate as gateways by simply relaying data from or to neighbouring nodes. Simulation results show that the introduction of the protocol drastically increases the volume of carried traffic on the network due to its coverage extension capabilities. Moreover, they show that the implemented power saving mechanism works as expected, introducing a series of configuration parameters to be taken into account in the design process of wireless mesh networks using this protocol.

Its design has been as generic as possible, so it can be applied to any client-server communication system, from a conventional wireless local area network (WLAN, WiFi) to a mobile phone network or even a WiMAX link. In this sense, although radio technology is not part of the protocol itself, tests and simulations present in the article were conducted using WiFi technology.

Several important advantages arise from its flooding nature (already explained in Section IV.A, e.g., an increased reliability or better self-reconfiguration and self-healing features, etc.), but the extensive use of these techniques could incur excessive energy consumption for the nodes' batteries, which would be compromised. For this reason, the implementation of an efficient power saving mechanism in the protocol itself is of vital importance to minimize the impact of its potentially energy-consuming nature. In this way, the main idea consists of reaching a compromise between energy savings derived from neither having to route nor to process data packets by the nodes, and the extra number of (re)transmissions derived from using such a flooding mechanism.

Keeping all this in mind, it is obvious that this protocol would not be suitable for every possible application since its battery requirements are quite high, but there are many scenarios (where batteries are not the network's bottleneck) in which this protocol could be perfectly used to exploit all its potential advantages over a normal WMN's protocol, e.g., in terms of carried traffic improvements, increased robustness or coverage extension, amongst many others. For example, this protocol could be very useful for mobile phone companies since although it is common for their networks to reach 80% of coverage quite easily, increasing that coverage area to 95% becomes a very difficult and expensive task. In this sense, it is very common to find small specific locations in urban areas with no coverage (due to signal fading effects when propagating through irregular metropolitan areas); however, a short distance from these areas is excellently covered. In these cases, the perceived quality of service of users (*QoE, Quality of Experience*) near that area could be very low. The fact of using the protocol described in this paper could provide a "virtual coverage" to users in a totally transparent way, avoiding such unwanted situations.

ACKNOWLEDGMENT

This research was supported by project grants CALM TEC2010-21405-C02-02 (TCM subprogram) and it was also developed under the framework of "programa de becas asociadas a la realización de proyectos en I+D, innovación y transferencia de tecnología 2009, de la Fundación Séneca, Agencia de Ciencia y Tecnología de la RM, (exp. No 10621/BPS/09)", and "Programa de Ayudas a Grupos de Excelencia de la Región de Murcia, Fundación Seneca".

REFERENCES

[1] F.-M. Zou, T.-S. Wang, X.-H. Jiang, and Z.-X. Lin, "A banyan-tree topology based railway wireless mesh network architecture," Tiedao Xuebao/Journal of the China Railway Society, vol. 32, no. 2, pp. 47-54, April 2010.

[2] Z. Yu, X. Xu, and X. Wu, "Application of wireless mesh network in campus network," 2nd Int. Conf. on Communication Systems, Networks and Applications, ICCSNA'10, vol. 1, pp. 245-247, 2010.

[3] N. Ghazisaidi, K. Hossein, and M. S. Bohlooli, "Integration of WiFi and WiMAX-mesh networks," 2nd Int. Conf. on Advances in Mesh Networks, MESH 2009, pp. 1-6, 2009.

[4] H. Wu, C. Qiao, S. De, and O. Tonguz, "Integrated cellular and ad hoc relaying systems: iCAR," IEEE JSAC, vol. 19, no. 10, 2001.

[5] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "UCAN: a unified cellular and ad-hoc network architecture," in ACM MOBICOM, 2003.

[6] S.-H. Kim, D.-W. Kim, and Y.-J. Suh, "A cooperative channel assignment protocol for multi-channel multi-rate wireless mesh networks," Ad hoc Networks Journal, vol. 9, no. 5, pp. 893-910, Jul. 2011.

[7] S. Pediaditaki, P. Arrieta, and K. M. Mahesh, "A learning-based approach for distributed multi-radio channel allocation in wireless mesh networks," Int. Conf. on Network Protocols, ICNP'09, IEEE Computer Society, pp. 31-41, 2009.

[8] D.-W. Kum, J.-S. Park, Y.-Z. Cho, B.-Y. Cheon, and D. Cho, "Mobility-aware hybrid routing approach for wireless mesh networks," Proceedings, 3rd Int. Conf. on Advances in Mesh Networks, MESH 2010, pp. 59-62, 2010.

[9] F. Martignon, S. Paris, and A. Capone, "A framework for detecting selfish misbehavior in wireless mesh community networks," Proceedings, 5th ACM Int. Symp. on QoS and Security for Wireless and Mobile Networks, Q2SWINET'09, pp. 65-72, 2009.

[10] K.-H. Lee and C. S. Hong, "A PKI based mesh router authentication scheme to protect from malicious node in wireless mesh network," Management Enabling the Future Internet for Changing Business and New Computing Services, pp. 405-413, 2009.

 ISBN: 978-1-61208-147-2