# Design of a UMTS/GPRS Assisted Mesh Network (UAMN)

J. Paradells[1], J.L. Ferrer[1], M. Catalan[1], W. Torres[1], M. Catalan-Cid[1], X. Sanchez[1], V. Beltran[1], E. Garcia[1], C. Gomez[1], P. Plans[1], J. Rubio[2], D. Almodovar[2], D. Rodellar[3], N. Subotic[3], D. Wenger[3], I. Steiner[3]. *Technical University of Catalonia[1], Spain. Vodafone R&D[2], Spain. SwissCom Innovations[3], Switzerland.*

***Abstract*** **Wireless Mesh or multi-hop networks (WMNs) are well known thanks to its simplicity on deployment and the lack of infrastructure. These two advantages come with some drawbacks. WMNs have limitations with the support of Quality of Service (QoS), they do not assure coverage or even connectivity, and security, management and monitoring are not considered key requirements. In order to benefit of mesh networks and use them as an operator graded network, it is necessary to either improve mesh networks to fulfill all these requirements or use an alternative network that offers full availability, connectivity and security to assist the mesh network. Considering the two options, the second is the one selected making use of GPRS/UMTS as an assistant network.**

**The document describes a set of requirements and the design of the functionalities needed to build an operator graded network using the cellular GPRS/UMTS. The aspects covered in the design are: security, quality of service, mobility, self configuration and optimization. The last point, optimization, is not directly involved with mesh networking, but it is an improvement easy to achieve when using a gateway node to access the Internet through a GPRS/UMTS connection. The design of the solution not only considers functionality, but also feasibility employing of the shelve elements. The mesh nodes and gateways are built on top of Linux operating system with the aim to reuse previous results and open source software. The final objective of the project is to build a usable system to be used as a proof of concept.**

***Index Terms*— WMN, Cellular Assistance, Heterogeneous Network, UAMN**

## I. Introduction

MESH or multi-hop networks are well known from long time ago. Nevertheless, they have keep being used in niche applications such as military or emergency networks. Only recently, thanks to the availability of high speed radio interfaces and the further development of microprocessors, it has been possible to develop nodes suitable for a massive deployment. These nodes can be associated to a person, object, sensor or actuator. In addition, to transmit and receive information from the user itself, the node should be able to relay transmissions from other nodes. This capability allows building a network with very interesting characteristics:

--The required transmission power is lower that the one required by one hop networks.

--There may be alternative paths to overpass obstacles.

--The network does not require infrastructure and, in this way, it is very robust and easy to deploy.

--The network is able to accommodate new nodes and react in front of vanishing nodes; as a result the network is even able to support mobility and nomadicy.

Wireless Mesh Networks (WMNs) have been used by the army or in emergency situations (e.g. after the hurricane Katrina) due to their robustness and easy deployment. Also, community networks use mesh concepts to skip ownership and operators. These examples do not envisage any commercial exploitation, but even thought it has seen interesting to study the possible usage of cellular networks to overcome the limitations of mesh networks which mainly include security and QoS issues [1]-[2]. To summarize, the main idea behind the project is to build a UMTS/GPRS assisted mesh network (UAMN).

The rest of the document is organized as follows. Section II presents the architecture of the network and lists the requirements in terms of security, mobility, QoS, self-configuration and protocol optimization techniques. Section III justifies the different design decisions and describes the proposed functionalities to implement in the network considering the different areas mentioned above. Finally, conclusions and future work about new challenges to be overcome are presented.

## II. UAMN Overview

### *A. Architecture*

The network is built with on purpose nodes able to work as access points and link to other nodes using a different air interface, IEEE 802.11b/g based standard for the access interface and IEEE 802.11a for the backhaul. The mesh network supports traffic among users attached to it or between a user and a device located in the Internet. This functionality requires the use of a gateway node, which is a mesh node with an interface to the cellular network (UMTS or GPRS) or the wired network (Ethernet, xDSL). Fig. 1 shows an example of the network.

The UMTS/GPRS network offers wide coverage and a trusted relation with the user. These two features allow solving the main drawbacks of mesh networks. The UMTS/GPRS network can be used to connect different parts of the same mesh network, manage nodes and monitor the performance of the mesh nodes deployed.

UMTS/GPRS offers security mechanisms that allow authenticating and authorizing a user as well as a new mesh node (MN). In addition, the accounting facilities available for GPRS/UMTS can be applied to mesh traffic.

User devices and MNs may have a cellular connection in addition to the WLAN interface. This is not a hard requirement on the design but, if present, it simplifies the configuration and allows the network to offer the best performance. The cellular connection is used by the user and the mesh nodes for signaling transport, and it may be used by the gateway (GW) nodes for data and signaling traffic. We understand for 'network signaling data' all the messages related to user's authentication, accounting and management. The routing signaling information is transmitted only using the wireless mesh interfaces. In mesh networks, more than one gateway node may be available to increase the robustness and the bandwidth of the interconnection. It can be seen that, even if several gateways are used, the UMTS interface may be the network bottleneck. To mitigate this problem the gateway nodes offer traffic optimization functionalities to reduce the traffic through the UMTS/GPRS interface. Each gateway is paired with a central proxy that helps with the traffic optimization. In this way, the protocols used between the proxy and the gateway can be modified to compensate the radio interface limitations.

As the intention was to build a working network with a limited effort in terms of time and resources, the design was based on off-the-shelf elements. The MN should be able to offer multiple WLAN interfaces (at least two, one for access and one for the backhaul) and one interface for the UMTS/GPRS connection. The Access Cube from 4G Systems has been selected as a mesh node, but there are several alternatives in the marked. This device uses an embedded Linux OS and offers enough memory and processor capacity to perform the mesh node tasks. The gateway has further functionalities (mainly in terms of traffic optimization) and requires a better hardware in terms of connectivity (for example, PCMCIA interfaces for High Speed Downlink Packet Access, i.e., HSDPA, cards) and processing power. Thus, the selected device is a PC running Linux.

The development of the project is intended in two phases. The first one has to find solutions to the different requirements of the UAMN. The second phase consists on selecting and integrating the different solutions coming from the first part of the project.

## B. *Requirements*

### 1) *Security*

As the mesh network can be seen as an extension on the UMTS/GPRS network, the UAMN should offer network authentication and privacy to the user and user authentication and authorization to the network operator. Also, mesh nodes must be authenticated, and routing information should be sufficiently protected in order to prevent malicious nodes to introduce erroneous information about routes. Additionally, the network should provide self-security mechanisms that react in front of attacks detection (e.g., changing functional parameters or avoiding certain routes).

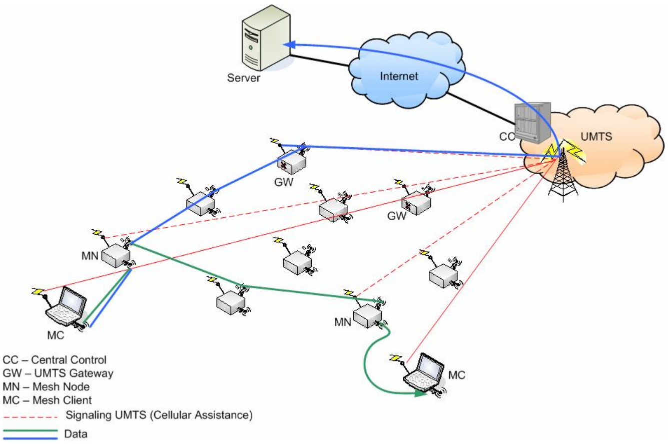

Fig. 1. UMTS/GPRS Assisted Mesh Network Architecture.

### 2) *Mobility*

User nodes connected to the UAMN should be able to move between mesh nodes as if these were simple access points, but they should support the security features listed above. Therefore, when an authenticated user associates to a new mesh node, no re-authentication should be needed. In addition, as the UAMN network must be compatible with the major part of wireless clients, no modifications at layer-2 should be done in the client side in order to reduce the layer-2 IEEE 802.11 handover process. However, the IEEE is working on the definition of new standards to solve this, like 802.11r and 802.11k.

### 3) *Quality of Service (QoS)*

For the same reasoning applied to the security requirements, the UAMN should provide quality of service in a similar way as it is provided by the UMTS/GPRS network, but with the additional problem of the mesh node mobility and the usage of an unlicensed band. The quality of service mechanisms are implemented in mesh nodes and gateways, where the different traffic flows should be transmitted using different paths and the appropriate link quality metrics used in the routing protocol. In order to distribute the traffic efficiently between gateways and perform an adequate admission control, nodes should periodically report information like load conditions and link capacity estimation of the WLAN or UMTS/GPRS interfaces in the case of the gateway nodes.

### 4) *Self-configuration*

The main advantages of the mesh network are its easy deployment and self-healing capabilities. A node should acquire its operational parameters from a server and by learning from the information provided by the surrounding nodes. The self-configuring mechanism should provide capabilities for selecting the most appropriate channel to use as we are working on an unlicensed band.

### 5) *Protocol optimization*

As it has been indicated the mesh network can be connected to the Internet using gateway nodes. It has been seen that the GPRS or even the UMTS interface introduce some bad effects on chatty protocols such as Hypertext Transfer Protocol (HTTP) due to long Round Trip Times

(RTTs) [3]. HSDPA will improve the performance of UMTS with higher speeds and shorter RTTs; however the chatty applications, such as web browsing, may still lead to delays [4]. This behavior degrades the performance of the transmission. This problem can be mitigated with the usage of optimized protocols through the radio interface. On a terminal directly connected to GPRS, UMTS or HSDPA this optimization requires to install software on the user device. However, in the proposed architecture this functionality can be located on the GW, which requires minor changes (without affecting the user devices).

## III. UAMN Design

The proposed solution offers its maximum benefits when users and MNs have a GPRS/UMTS connection. This is not a strict requirement and the mesh network can be built and used even if the GPRS/UMTS network is not available. The description of the design is done considering the usage of fully equipped nodes.

### *A. Security*

Security in the UAMN can be divided in three parts: the authentication and authorization phase, the data protection mechanisms and the integrity of the routing protocol messages.

#### *1) User authentication and authorization phase*

First of all, assuming that the user has a cellular interface, the mobile client is authenticated by the operator's cellular network and gets IP connectivity. By means of the cellular interface, the user authenticates again as a mesh user to the Central Control (CC) that will have a Remote Access Dial-In User Server (RADIUS) as an Authentication, Authorization, and Accounting (AAA) system. In an operational system one single authentication may be enough to gain access to the service. Once the user is authenticated the CC provides the WLAN interface configuration information to connect the terminal to the WMN using the UMTS/GPRS interface.

The network sends to the user the MN acting as an access point (AP), i.e., to which MN the user must associate. Thus, at this point, a QoS mechanism takes place to decide which MN has the best conditions for the user association. This mechanism is described in section C.1) and it is mainly based on reporting to the central entity measurements about the surrounding MNs and other interfering WLAN networks.

Just after the selection of the MN, the CC transmits the security keys via the UMTS/GPRS network, taking advantage on the secure nature of this link. This key is utilized to cipher information via the WLAN link, between the user and the MN. Therefore, the CC sends the key and the user security context information to the MN too. In addition, the surrounding mesh nodes that the user has previously sensed and reported to the CC also receive the same security context information. As a result, when the user moves from one MN to another, no re-authentication phase is needed. This approach is similar to the technique proposed in [5], where it is demonstrated how the handoff time can be reduced.

#### *2) Backhaul security*

The mesh interface (i.e. 802.11 interface which works in ad-hoc mode for connecting with other mesh nodes) has a lack of actual support of data encryption at layer 2. In fact, most open source driver implementations and security solutions in 802.11 networks are centralized and based in managed mode. As a result, additional security has to be implemented in higher Open Systems Interconnection (OSI) layers. In that case, the most suitable mechanism is to apply security at layer 3 using IPsec. The traffic between MNs and GW is protected with IPsec tunnels. . If other network equipment with layer 2 encryption support is used to build the WMN, the same security solution can be utilized and, consequently, the security in the backhaul is increased.

Security keys may be distributed via the UMTS/GPRS interface, where the CC acts as the centralized element that distributes the keys, controlling the validity time and updating them when needed. Using this information, the mesh nodes can authenticate other nodes and encrypt the connection.

#### *3) Routing protocol security*

Several proposals for security in Mobile Ad-Hoc Networks (MANET) routing protocols exist, as Secure Optimized Link State Routing Protocol (SOLSR) [6] or Secure Ad-Hoc On-Demand Vector (SAODV) [7]. Despite the fact that not all the implementations are available and others are only a theoretical approach, there is a security plug-in available for the OLSRD [8] implementation that signs the routing protocol control packets avoiding malicious information introduced in the network by unfriendly nodes. Nevertheless, a similar signature mechanism can be applied to current AODV implementations, which will provide the data integrity necessary in the routing protocol information messages.

Either OLSR or AODV routing protocol implementations can be utilized as a routing protocol in the mesh network. However, for our proof-of-concept prototype we have decided to make use of the AODV-ST implementation [9] with some modifications due to the next reasons:

--Possibility of using diverse link quality metrics with minor changes.

--In has a built-in Spanning Tree protocol to work with several GWs. Thus, it is possible to maintain information about GWs in the MNs.

--Digital Signature of the routing data packets has been also implemented with minor changes.

### *B. Mobility*

The mobility functionality works in conjunction with the security proposal because the same IP tunnel is utilized to maintain mobility and for data encryption. This approach reduces the total IP header overhead. Also, note that MNs mobility is supported thanks to the ad-hoc routing protocols used in the backhaul.

The handoff procedure in WLAN networks suffers from gaps produced by layer-2 and layer-3 delays. There exists several proposals in the literature that provide less handoff time by means of modifying the client driver software; because the major delay time is included in the AP probe phase. For example, authors in [10] provide fast handoff and fast re-authentication using neighbor graphs for caching client information and providing an optimized list of APs to the clients.

Due to the fact that reducing layer-2 handoff time requires software modifications at low levels, the mobility solution used is based on minimizing the layer-3 handoff time. In essence, it uses an extension of the hierarchical mobile IP solution. When exchanging traffic with the Internet the gateway has the role of Mobile Anchor Point (MAP) and the mesh node (MN) where the user is connected acts as the foreign agent. Layer-2 triggers [11] when a user is associated to a new MN and then the tunnel is created if it is not already available for another connection.

This centralized approach of mobility provides control of all the traffic in some specific points, i.e. the GWs, to the operator. Therefore, monitoring the traffic in the GWs is possible to implement usage control mechanism, admission control or even accounting functions. However, this is not optimal for internal communications due to the fact that the traffic follows always the same paths passing through the gateways. For example, if two users are associated in neighbor MNs and want to establish a communication, all traffic will be forced to pass through each user's assigned GW.

As a consequence, another possibility to support user's mobility is to define a distributed architecture, where the IP tunnels are also created between MNs, not only from MNs to GWs.

### C. *Quality of Service*

The quality of service mechanisms are implemented in mesh nodes and gateways. The proposed solution for supporting QoS starts when a user wants to gain access to the network and its applied during all the time the mobile client is using the mesh network The different traffic flows are classified according to the IP address fields and ports, and each category is routed using a specific link quality metric.

#### 1) *User mesh node and gateway assignment protocol*

The terminal contacts with the central control and provide identities and Signal-to-Noise Interference Ratio (SNIR) of each access point (AP) available. The central control decides the best suited mesh node using available measures [12] and notifies the decision to the terminal and the selected mesh node. These measurements not only include the nearest nodes that belong to the mesh network but also the measurements from external WLAN cells. All this information is utilized by the CC to get statistics about coverage and perform frequency allocation and transmission power adjustment.

Note that with all these information the user:

--Gives a list of all possible APs from other networks that are causing interferences, which can be used in the CC for the frequency allocation algorithm.

--Provides a list of APs that belong to the operator (i.e., the MNs) which are candidates to receive a handover when the client moves from one MN to another. This information can be used for sending the authenticated client information to these neighbor MNs to minimize the handover time. This list is also useful to perform load balancing when associating to a mesh network.

With this information the CC should choose a MN from the list with a good SNIR and enough empty capacity to accommodate the QoS requirement of the new user. Then, the CC sends a response to the client with the SSID, channel, encryption key and MAC address of the MN (in addition to the IP addresses and GW address for the client's WLAN interface configuration).

The gateway assignment protocol is a proposed functionality that is implemented mainly in the CC, which is the element that knows all the information about the active connections in the network, the users assigned to the different GWs and MNs, and also, the capacity estimation at the different gateways present in the network. Thus, when the user has been authenticated and authorized, the CC calculates the gateway priorities based on the parameters mentioned above. The CC generates a GW priority list which is transmitted to the MN where the user is associated. The MN combines this information with the local node information (i.e., routing metrics) about the GWs in order to select the most appropriate gateway for the user. Once the GW is selected, the MN sends the user's selected GW via UMTS/GPRS and redirects all the outgoing traffic from the user to the specific GW.

#### 2) *Link capacity estimation*

UMTS links, mainly in upstream direction and compared to other Internet access technologies, provide lower capacity. The bit rate of a UMTS access may vary in time (fading, increment of users, etc.), especially considering the possibility of gateway mobility. So, a periodical estimation of the gateway/UMTS link capacity will be necessary.

There are two well known TCP/IP techniques to estimate the capacity of a link: Variable Packet Size (VPS) and pairs of probe packets [13]. The first method basically sends a group of ICMP packets of different sizes in each interval and measures the RTT of each one. It assumes that the minimum RTT (for every size) will correspond to a packet that has not find congestion through the link, so it will give the nominal capacity of the link.

Packet-pair methods are based on sending two consecutive packets of different length, first a short packet and then a larger one. Sending first a short packet minimizes the probability of suffering cross-traffic between the pair, which can lead to subestimation (measured delay is incremented). On the other hand, the large packet maximizes the probability of processing the short packet on the neighbor node before the large arrives, since if there is cross-traffic and the short packet must wait in the queue, the delay can be decremented, leading to overestimation.

The same methods described above are applicable to the estimation of the WLAN links between MNs. This information can be available at the CC, periodically reported by the MNs via the UMTS/GPRS interface. The estimated value can be used in link metrics optimization, interferences detection or mal-function of some nodes. Therefore, we decided to integrate in the routing protocol a packet pair technique to estimate the link capacity between mesh nodes. The packets characteristics are:

--Short packet Data: 32 bytes; IP and UDP Header: 28 bytes; Total: 60 bytes.

--Large packet Data: 360 bytes; Padding: 1104 bytes: IP and UDP Header: 28 bytes; Total: 1492 bytes.

First experiments have demonstrated that the estimated values are similar to other more sophisticated bandwidth measurement tools.

*3) Traffic classification and scheduling*

The proposed solution assumes there are three traffic classes and nodes treat them differently using different routing metrics and scheduling rules at the mesh nodes. Traditionally, the number of hops has been used as routing criteria in fix networks to decide the best path from source to destination. In mesh routing the uncertainty in the link performance and the availability of multiple paths from source to destination promote the usage of routing metrics based on packet error rate and available bandwidth. In addition, the usage of non-discrete metrics allows soft reconfiguration when a mesh node is moving.

The possible routing metrics can be computed in parallel in the same routing protocol, thus, the routing protocol can have different paths depending on the different metrics applied (minimum number of hops, Expected Transmission Time (ETT), Expected Transmission Count (ETX) or combination of both) [14]. The three defined traffic classes correspond to background, bandwidth assured and real time.

Fig. 2 depicts the routing process using multiple link quality metrics, one for each routing table since Linux kernel allows the usage of multiple routing tables. The classifier sets the corresponding Type of Service (ToS) field, while the Routing Table Marker sets a label to the IP packet that identifies which kernel routing table must this packet use.

As different traffic flows from one user may pertain to different service classifications, the routing tables vary for each type of traffic. In consequence, different virtual IP tunnels exist from one destination to another, each with different treatment at each mesh node according to the traffic class.

### D. Self-Configuration

The self-configuring capabilities in the network nodes are firstly centered on the selection of the best radio channel according to interference conditions.

First of all, we have to take into account that in the long term, we may use solutions provided by current standardization efforts. The 802.11s group is creating a standard that will provide mesh features to APs: they will be capable of forwarding data using multi-hop transmissions; the future 802.11k and 802.11v standards will enhance management by adopting new measurements and information exchange across layer 2 mechanisms. In a similar way, the current 802.11h amendment [15] offers useful mechanisms for frequency and power management in order to avoid interference with other systems. Also IEEE 802.11f standard [16] recommends the use of Inter Access Point Protocol (IAPP) to provide communication between APs, but since it is mainly focused on the roaming of mobile users and also requires layer 3 mechanisms to route its packets, it will not be considered.

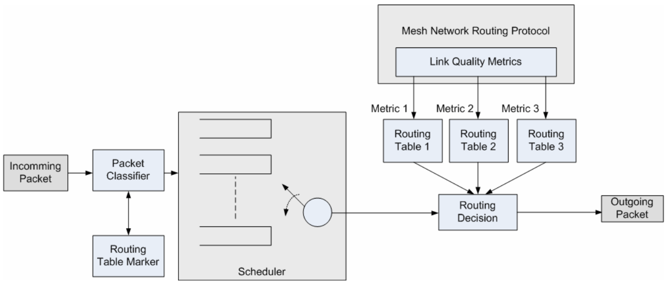

Fig. 2. Traffic Classifier and Packet Scheduler Scheme.

Following a different approach, IETF CAPWAP Working Group focuses its efforts in developing a standard for control and provisioning of APs, based on the ideas of LWAPP protocol [17]. LWAPP aims to redefine the concept of AP by transferring part of the AP's logic to a centralized Access Controller from which many of these light APs are managed.

The availability of a GPRS/UMTS interface simplifies the acquisition by the CC and the distribution of configuration information. In particular, it is possible to utilize the CC to coordinate the frequency used by the radio access interface on each mesh node.

The channel allocation algorithm we propose is inspired by DSATUR [17] applying the idea proposed in [18] and [19] of adding a certain cost. Thus, this is an algorithm to color the vertices of a graph based on a degree of saturation that is calculated from a certain cost.

The DSATUR algorithm establishes the order in which nodes must be colored and the colors (i.e. non-interfering frequencies) to assign. At each of the iterations, the node with a higher saturation degree (i.e. the node with a larger number of colored neighbors) is selected to be colored. If more than one node has the same saturation degree, the one with the highest ordinary degree (i.e. the node with the largest number of neighbors) is selected, if the draw persists, then a random selection is performed. Since the assignment may be computed on different devices and all of them must obtain the same result, all nondeterministic steps must be replaced; e.g. ties can be broken using the physical address of the nodes. The color assigned to the selected node is the lowest channel not being used on any of its neighbors.

When there is a great density of nodes and edges (e.g. imagine a subset of four vertices, where each vertex is connected with the other three, i.e. a clique of 4) and we have just 3 colors (i.e. 3 non-overlapping channels), this algorithm is not useful since it tries to solve a problem

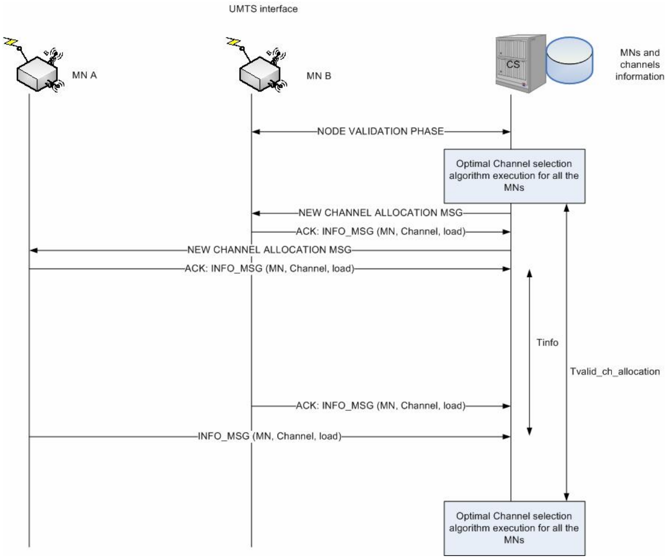
UMTS interface
MN A
MN B
CS
MNs and channels information
NODE VALIDATION PHASE
Optimal Channel selection algorithm execution for all the MNs
NEW CHANNEL ALLOCATION MSG
ACK: INFO_MSG (MN, Channel, load)
NEW CHANNEL ALLOCATION MSG
ACK: INFO_MSG (MN, Channel, load)
Tinfo
Tvalid_ch_allocation
ACK: INFO_MSG (MN, Channel, load)
INFO_MSG (MN, Channel, load)
Optimal Channel selection algorithm execution for all the MNs

Fig. 3. Sample of Frequency Allocation Protocol Messages Interchange.

when there is no feasible solution. If we use all existing channels (13 in Europe), we will obtain feasible solutions for almost every actual scenario, but as stated before, if we use overlapping channels in interfering cells, we will suffer a degradation of the performance. For that reason we introduced some modifications on the algorithm with the aim of minimizing interferences to MNs with heavy traffic.

The concept of saturation degree is modified including the weighted interference of a node seen from its neighbors.

The CC can coordinate the channel allocation in the network when external interferences are reported by the user authentication phase or any link degradation is detected. Also, MNs report measurements from its neighbors in a similar way on the user authentication phase. This takes place when a MN is activated and validated against the CC via the GPRS/UMTS interface. Just after the MN validation, the CC sends a message to the MN with the channel assignment information. Fig. 3 describes the different messages that are going to be interchanged via UMTS/GPRS between the MNs and the CC when MN B is joining the WMN:

--INFO_MSG: Periodically message reported every Tinfo seconds by the MNs including information about the current channel, MN identification and load conditions in the access channel.

--NEW CHANNEL ALLOCATION MSG: Message with the channel assigned to the MN that is transmitted by the CC to all MNs every Tvalid_ch_allocation seconds.

### *E. Protocol optimization*

Current UMTS networks use dedicated channels (DCH) for transmissions offering up to 384 kbps in downlink and either 64 kbps or 384 kbps in uplink. In terms of delay, [20] reports RTTs measured using the ping tool that range from 200 ms to 450 ms depending on the packet sizes. Furthermore, throughput may be acceptable for deploying services such as video streaming. In terms of delay and throughput, HSDPA improves the performance of UMTS; thus is can be expected that the services that can be deployed under UMTS would perform better over HSDPA.

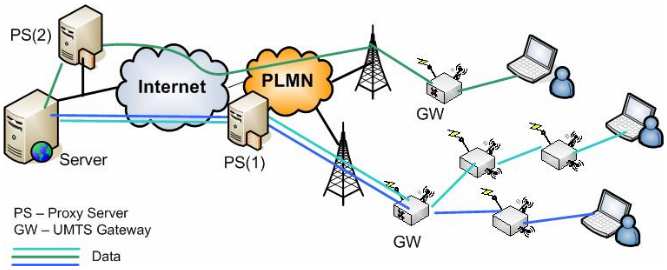

Fig. 4. UAMN Proxy Approach for Protocol Optimization.

However, it should be taken into account, that the performance of other applications, such as web browsing, may be degraded in UMTS and HSDPA due to three reasons:

--Handover events and link outages, which cause packet losses and connectivity gaps.

--Bandwidth asymmetry. Current HSDPA networks support up to 1.8Mbps in the downlink and 384kbps in the uplink. For instance, in HTTP transmissions requests are sent at low rates, which cause significant transmission delays prior to downloading objects.

--Protocol-incurred inactivity times. Communications based on the Transmission Control Protocol (TCP) suffer from idle periods due to the initial connection establishment and the slow start phase. UMTS delays lead also to a significant inactivity due to the Domain Name Service (DNS) resolution process. On the other hand, web downloads are especially affected due to the default HTTP Request-Response mechanism [21]. The browser requests an object and must wait until the complete reception of this object before sending a new request. This behavior induces a stop and wait pattern. Since downlink transmission delays in UMTS and HSDPA are short in comparison to idle periods, the HTTP stop and wait pattern leads to the underutilization of the link.

The proposed design relies on two elements (see Fig. 4):

--The UMTS/GPRS Gateway (GW). As the GW acts as the link between the WMN and the UMTS/GPRS network, it is a strategic node to carry out access control or addressing mechanisms. Furthermore, connections to the public server are split in the GW. By this way, particular problems of the WMN and the cellular network can be optimized separately.

--A proxy located in the wired network either i) as part of the mobile operator's infrastructure (labeled as PS(1) in Fig. 2) or ii) as a component of a private network connected to Internet (labeled as PS(2) in Fig. 4). From now on we will refer to this device as Proxy Server (PS). The usage of a proxy to improve the perceived performance is quite common for mobile operator, and different mechanisms (such as content adaptation) may be carried out at the PS prior to the transmission of information through the UMTS/GPRS network.

The combination of a network proxy (the PS) paired with the GW at the other end of the UMTS/GPRS interface opens a wide range of new optimization possibilities. We can define any kind of mechanism or protocol between the PS and the GW in order to solve the specific problems of

TABLE.I.
WEB DOWNLOAD AVERAGE AND NORMALIZED TIMES FOR THE CNN WEB PAGE AND SEVERAL OPTIMIZATION METHODS.

| | | Default HTTP Header | | | | | HTTP Header Reduction | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 2 conn. | 8 conn. | Pipelining | Pipelining 8req | Single file | 2 conn. | 8 conn. | Pipelining 8 req | Single file |
| HSDPA | Time (s) | 9.067 | 4.892 | 5.733 | 5.314 | 1.489 | 7.219 | 3.320 | 4.063 | 1.555 |
| | Normalized | 1.000 | 0.540 | 0.632 | 0.586 | 0.164 | 0.796 | 0.366 | 0.448 | 0.171 |
| UMTS1 | Time (s) | 14.459 | 8.254 | 8.073 | 7.627 | 5.393 | 11.705 | 6.261 | 6.965 | 5.004 |
| | Normalized | 1.000 | 0.571 | 0.558 | 0.528 | 0.373 | 0.809 | 0.433 | 0.436 | 0.381 |
| UMTS2 | Time (s) | 15.22 | 10.54 | n.a. | n.a. | 8.34 | 13.38 | 9.03 | n.a. | 7.6 |
| | Normalized | 1.000 | 0.821 | n.a. | n.a. | 0.491 | 0.877 | 0.619 | n.a. | 0.477 |
| WLAN | Time (s) | 1.376 | 1.385 | 1.411 | 1.394 | 0.309 | 1.365 | 1.384 | 1.499 | 0.320 |
| | Normalized | 1.000 | 0.992 | 1.013 | 1.003 | 0.232 | 0.983 | 1.001 | 1.023 | 0.228 |

the UAMN network. Concretely, our proposal relies on several solutions that cover different layers. Some of these methods could be combined or applied individually depending on the needs and capabilities of the target scenario.

We have evaluated several optimization methods to improve the performance of web browsing over UMTS/GPRS networks, which can be applied in the communication between the GW and the PS:

--HTTP/1.1 mechanisms. The GW could support pipelining or open multiple simultaneous for a single transmission to improve the utilization of the UMTS/GPRS/HSDPA link. Otherwise, the GW can aggregate the traffic of several users that access the Internet through it; in this case, the performance obtained by traffic aggregation would be similar to the usage of multiple simultaneous connections. In the trials, pipelining mechanism was enabled/disabled. Furthermore, the maximum number of pipelined requests was set to 4 (default case) and 8 (maximum value). The number of simultaneous connections was also set to 2 (default case) and 8.

--HTTP header reduction [23]: To minimize the size of the HTTP requests in the uplink, the redundant information was removed from the headers. In the above-mentioned design, this mechanism would be performed by the GW. By the way, the PS should be aware of the original headers and reconstruct them before sending the information to the server.

--Single file approach [23]: All the objects were bundled in a web page downloaded as a single file. It must be noted that in the trials we only evaluate the transmission time of the information. In the proposed approach, the PS would be responsible to bundle the objects in a single file before the download and the GW would perform the unbundling and delivery to the web client, what would imply an additional processing time.

Table I illustrates some of the results obtained for the download of a web page. In these tests, a laptop connected to Internet through a wireless interface downloads the CNN web page reproduced on a web server located on the university campus network in order to prevent server loads. In this case, the laptop emulates the mechanisms that can be implemented in the GW and the local server emulates the PS. UMTS1 and UMTS2 networks belong to two different mobile operators. The UMTS1 network scenario supported 384kbps in the downlink and in the uplink. On the other hand, the UMTS2 network supported only 64kbps in the uplink and implemented dynamic bandwidth allocation in the downlink [22]. Finally, WLAN trials were performed with an IEEE802.11b interface. All the results have been normalized to the default case in most commercial browsers (i.e. 2 simultaneous connections per server and pipelining disabled).

Results show that HTTP/1.1 mechanisms improve the performance of web downloads over HSDPA and UMTS, but they do not completely mitigate the underutilization of the link. As it can be observed, a simple HTTP header reduction [23] can lead to a substantial throughput improvement in the case of UMTS or HSDPA and can be used in addition to other optimization methods (e.g. pipelining or the usage of multiple simultaneous connections). Since this technique reduces the transmission time of the uplink packets, its benefit is more notable in networks that suffer from a high bandwidth asymmetry such as HSDPA. Furthermore, this method saves the transmission of around 9% of all information exchanged.

The single file approach leads to the best results since it maximizes the utilization of the cellular link. It should be noted that, in this case, the results obtained for HSDPA are close to the performance of a WLAN connection. Thus, if this technique is implemented between the GW and the PS, the total web download time from a mesh client going through the HSDPA network could be reduced to few seconds, what would notably improve the end user perception.

Further optimization techniques such as DNS cache, file compression or TCP/IP optimization [20] can be also applied to the gateway approach.

## IV. CONCLUSIONS

Mesh networks are being considered as a cheap alternative to gain coverage and to provide broadband wireless connectivity. In the same manner they are easy to deploy, they are difficult to manage. The usage of an overlapping network such UMTS/GPRS to assist the mesh network tries to overcome the mentioned problem offering centralized support. The main idea is to provide the mesh network with a signaling plane available elsewhere and secure. This signaling should be responsible for transporting information related to the user, e.g. about authorization and quality of service, and also for exchanging management and monitoring information with the mesh nodes. From the point of view of user data, the mesh network can be isolated or connected to the fix network. The element between the two networks is the gateway. This element can be as simple as a mesh node, but it can accommodate additional functions to improve performance when the mesh is connected through a cellular interface such as GPRS, UMTS or HSDPA. This new concept of an assisted mesh network requires to be validated. For this purpose, a proof-of-concept prototype has been designed and it is being built. This prototype will be used first of all to adjust the behavior of the network and once optimized to validate the concept. To accelerate the construction of the prototype, the design has considered available software components and open platforms able to accommodate them. At the present phase, individual components for security, QoS or optimization have been tested satisfactorily and the integration is on the way.

## V. Future Work

The document has described all the design key issues for the reference scenario (see Fig. 1). However, there are some aspects that are not definitively closed, like the QoS treatment for each traffic flows or the handling of mobility. The assistance provided by the CC to the mesh network in order to offer QoS has to be adjusted. The approach uses information provided by mesh clients (MCs) and mesh nodes (MNs) to provide feedback related to channel assignment, routing and gateway selection. The exact algorithm used to decide this feedback and how it is going modify the behavior of the mesh network has to be determined. Once the prototype is built, it will be used to study different alternatives. The final approach will be affected by two limitations: the amount of information exchanged with the CC and the delay. It is clear that the amount of data through the UMTS/GPRS interface should be minimized. Furthermore, the delay introduced by the data transfer and processing at the CC will limit the usage of the feedback. The final decision on the assistance provided by the CC will result on a compromise between local decisions,, taken by the algorithms on the mesh network, and the global view of the CC. One possible response to this compromise is to allow the mesh taking quick responses but using criteria updated periodically by the CC.

For the mobility part, the two approaches (centralized and distributed) will be evaluated. The centralized one could be the easiest to implement. However, it could lead to a wrong use of one of the advantages of WMN, i.e. its distributed nature. However, the distributed approach adds more complexity in the MNs and in the management of active connections, due to the fact that all nodes are acting as a MAP in the Hierarchical Mobile IP architecture. Consequently, the two approaches should be evaluated taking into account in each case how they affect the network traffic distribution. Also, the handover delays should be measured and considered. Note that the distributed case can be seen as an extension of the centralized case.

## Acknowledgments

This work was supported in part by the i2CAT Foundation, Vodafone Research and Development.ES, FEDER, the Spanish Government through project TIC2003-01748, FSE and DURSI.

## References

[1] Ben Salem, N.; Hubaux, J.-P. “Securing wireless mesh networks”.Wireless Communications, IEEE. Volume 13, Issue 2, April 2006.

[2] Faccin, S.M.; Wijting, C.; Kenckt, J.; Damle, A. “Mesh WLAN networks: concept and system design”. Wireless Communications, IEEE. Volume 13, Issue 2, April 2006.

[3] C. Gomez, M. Catalan, D. Viamonte, J. Paradells, A. Calveras, "Web browsing optimization over 2.5G and 3G: end-to-end mechanisms Vs usage of performance enhancing proxies", Wireless Communications and Mobile Computing (to appear).

[4] J. Gozalvez, “HSDPA Goes Commercial”, IEEE Vehicular Technology Magazine, pp. 43-53, March 2006.

[5] Mishra, A.; Min Ho Shin; Petroni, N.L., Jr.; Clancy, T.C. and Arbaugh, W.A.”Proactive key distribution using neighbor graphs” IEEE Wireless Communications, Feb 2004.

[6] Fan Hong Liang Hong Cai Fu. ”Secure OLSR”. 19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005. 28-30 March 2005.

[7] M. Guerrero Zapata. Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing. IETF MANET Internet Draft. 5 September 2006. Avaliable on line at: http://tools.ietf.org/wg/manet/draft-guerrero-manet-saodv-06.txt

[8] Unik OLSR Implementation. Home Web Page : http://www.olsr.org

[9] AODV-ST Implementation. Home Web Page: http://www.cs.ucsb.edu/~krishna/aodv-st/

[10] C-C Tseng; L-H Yen; H-H Chang and K-C Hsu; “Topology-aided cross-layer fast handoff designs for IEEE 802.11/mobile IP environments”. IEEE Communications Magazine. Dec. 2005.

[11] John C. Lin and S. Rangarajan. “LIHP: A Low Latency Layer-3 Handoff Scheme for 802.11 Wireless Networks”. World of Wireless Mobile and Multimedia Networks (WoWMoM) 2006.

[12] E. Garcia, R. Vidal, J. Paradells, “Load Blancing in WLAN through IEEE 802.11k Mechanisms”, 2006. ISCC ’06. Proceedings. 11th IEEE Symposium on Computers and Communications, June 26-29, La Manga del Mar Menor, Murcia, Spain.

[13] C. Dovrolis, R.S.Prasad, M.Murray, K.C.Claffy “Bandwidth Estimation: Metrics, Measurement Techniques, and Tools” IEEE Network, November/December 2003.

[14] R. Draves, J. Padhye and B. Zill. “Routing in Multi-radio, Multi-hop Wireless Mesh Networks” In ACM MobiCom, Philadelphia, PA, September 2004.

[15] IEEE 802.11 WG. Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe, IEEE std 802.11h. New York, USA: The Institute of Electrical and Electronics Engineers, Inc., October 2003.

[16] IEEE 802.11 WG “IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation”, IEEE std 802.11f. New York, USA: The Institute of Electrical and Electronics Engineers, Inc., July 2003.

[17] P. Calhoun, B. O’Hara, et al., “Light Weight Access Point Protocol (LWAPP)." Internet-Draft, draft-ohara-capwap-lwapp-03, June 2005.

[18] Brélaz, D. “New Methods to Color the Vertices of a Graph”, Communications of the ACM, vol. 22, pp. 251-256, 1979.

[19] Costa, D. “On the use of some known methods for T-coloring of graphs”, Annals of Operations Research: vol. 41, pp 343-358, 1993.

[20] Gomez, C., Catalan, M., Viamonte, D., Paradells, J. and Calveras, A., “Internet traffic analysis and optimization over a precommercial live UMTS network”, In Proceedings of the IEEE 61st Vehicular Technology Conference. VTC 2005-Spring, 5 (Stockholm, Sweden, May 30, 2005), pp 2879-2884.

[21] John, H., Katia, O. and Joe, T., “Modeling the performance of HTTP over several transport protocols”, IEEE/ACM Trans. Netw., 5 (1997), 616-630.

[22] H. Holma, WCDMA for UMTS: Radio Access for Third Generation Mobile Communications (3rd Edition). John Wiley & Sons, Inc., 2004.

[23] M. Catalan, C. Gomez, P. Plans, J. Paradells, A. Calveras, J. Rubio and D. Almodovar, “Extending Wireless Mesh Networks over UMTS: A proxy-based approach”, Wimeshnets Workshop. Qshine’06, August 7–9, 2006, University of Waterloo, Ontario, Canada.