Management Issues on Wireless Mesh Networks

Jairo L. Duarte[†], Diego Passos[†], Rafael L. Valle[‡], Etienne Oliveira[†],
Débora Muchaluat-Saade[‡] and Célio V. Albuquerque[†]

[†]Instituto de Computação
Universidade Federal Fluminense
Niterói, RJ, Brazil

[‡]Departamento de Engenharia de Telecomunicações
Universidade Federal Fluminense
Niterói, RJ, Brazil

***Abstract*—Wireless Mesh Networks (WMN) are emerging as a flexible and low-cost alternative to provide digital inclusion through multi-hop communications, supporting applications from last-mile Internet delivery, search and rescue, home networking to distributed gaming. Managing increasingly large and unplanned WMNs has many challenges. This paper has the primary goal of raising management issues in wireless mesh networks. Furthermore this work documents the management solutions deployed by the ReMesh project [1] in terms of network configuration, topology view, access control, performance measurement and statistics.**

I. Introduction

Wireless Mesh Networks (WMN) are emerging as flexible and low-cost extensions of wired infrastructure networks. Specifically in developing countries such as Brazil, broadband connectivity through traditional xDSL and cable access networks are affordable to a handful. Alternative solutions such as extending the reach of traditional Wi-Fi hot-spots through the use of multi-hop wireless networks are attractive and have the potential and the appeal for digital inclusion. Wireless mesh networks (WMNs) [2] aim at guaranteeing connectivity despite medium adversities and user mobility. WMNs build a multihop wireless backbone to extend the coverage area of traditional infrastructure networks, interconnecting isolated LANs and providing backhaul access to users. The backbone is composed of wireless routers in charge of concentrating and forwarding data. Backbone routers are typically stationary and users are able to roam among them.

In October 2005, the Brazilian National Research and Education Network, RNP, launched a wireless mesh network working group named the ReMesh Project. In March 2006 the first WMN was deployed over the city of Niteri, RJ, and since then much interest in this solution has come out. In 2007, the ReMesh project has spawned three new networks over the cities of Brasilia, Curitiba and Belem. Similar initiatives have been happening all over the world and growth rate of WMNs is extraordinary. Typical WMN applications include last-mile Intenet delivery, search and rescue, home networking and distributed gaming.

[1]This work is supported in part by grants from CNPq, Faperj, RNP and TBE/ANEEL.

One recent trend is to include multi-hop communications capabilities into portable laptops. This approach was introduced by the One-Laptop-Per-Child (OLPC) project deploying the IEEE 802.11s draft and is now followed by other low cost laptop manufacturers. This initiative can accelerate even more the organic widespread of WMNs. Managing such large and unplanned WMNs has many challenges. By definition, "network management is a process of controlling a complex data network so as to maximize its efficiency and productivity" [21]. This process involves data collection, data processing, data analysis, and problem fixing. To accomplish this process, network management can be functionally divided into five areas: fault management, configuration management, security management, performance management, and accounting management.

The ReMesh workgroup has built a new set of tools, specifically designed to address daily management issues. Such tools are inspired by and in some cases extended from existing tools whenever the similarities with wireline and wireless ad-hoc networks can be exploited, such as the inherent WMN backbone and their link variability.

This paper has the primary goal of raising management issues in wireless mesh networks. Furthermore this work documents the management solutions deployed by the ReMesh project, in terms of network configuration, topology view, access control, performance measurement and statistics.

The remainder of this paper is organized as follows. Section II describes WMN initiatives and briefly describes their implementations. Section III presents the architecture of the ReMesh project. Section IV lists and raises challenges of managing WMN and how some of them are handled in the ReMesh project. Section V discusses on remaining open issues and finally, Section VI concludes this article.

II. Mesh Networks

Over the last years, several universities and research centers around the world have been developing and widely deploying intra-campus wireless networks for ubiquitous communication [15]. More recently, wireless technology has been used for providing access to campus networks for users living nearby, using the concept of mesh networks. There are several pilot

projects of mesh networks around the world. Examples are RoofNet at MIT [4], [9], VMesh in Greece [38], MeshNet at UCSB [16], [30], CUWiN in Urbana [23], Microsoft Mesh [11], [12], Google Mesh, ReMesh in Niterói [26], among others [39].

Besides academic projects, commercial solutions are already on the market, offered by huge enterprises such as Nortel [34] and Cisco [37] and several other small companies [5]. Several governments are investing on building digital cities using wireless mesh networks, such as in Dublin [39], in Taipei where Nortel equipments are used and recently in the historical city of Tiradentes in Brazil, which used the Cisco solution. One big disadvantage of commercial mesh routers is their cost, which is not affordable to ordinary end users. The ReMesh solution, such as in [4], [38], [16], [23], is linux-based, open-source and based on a low-cost wireless router.

Some solutions, including the ones from Microsoft [12], Nortel [34] and Cisco [37], use two different transmission frequencies, usually 802.11a 5GHz for the backbone (links between wireless routers) and 802.11b/g 2.4GHz for access links (links between end users and access points). Since in Brazil the 5GHz band in not regulated yet, ReMesh uses only the 2.4GHz band and, like RoofNet and VMesh, end users are connected to mesh access points through wired Ethernet or WiFi access.

In terms of the routing protocol, different solutions are chosen by each project. VMesh and ReMesh use OLSR (Optimized Link State Routing) [8], a standard pro-active routing protocol. Microsoft Mesh uses an on demand reactive source routing protocol derived from DSR (Dynamic Source Routing) [18], called MR-LQSR (Multi-Radio Link-Quality Source Routing) [12]. RoofNet developed a hybrid approach, combining link state and DSR-style on-demand querying, named Srcr [4]. The work presented in [30] from UCSB uses AODV (Ad Hoc On-Demand Distance Vector) [28], a standard reactive routing protocol. Ciscos solution uses a proprietary routing protocol named AWP (Adaptive Wireless Path) [37] and Nortel uses the traditional OSPF (Open Shortest Path First) wired routing protocol [34]. The CUWin project is developing a scalable link state routing protocol that minimizes the cost of maintaining a consistent view of the network, called HSLS (Hazy Sighted Link State) routing [5], [35], [36].

Link costs can be calculated using traditional hop-count [8], per-hop round trip time, packet pair delay [12], ETX (Expected Transmission Count) metric [9] or similar derived metrics such as ETT (Expected Transmission Time) [4] and WCETT (Weighted Cumulative Expected Transmission Time) [12]. ETX dynamically measures link quality to find best routes. The ETX of a link is calculated using the forward and reverse delivery ratios of the link. The delivery ratio is the probability that a data packet successfully arrives at the next hop. The expected probability that a transmission is successfully received and acknowledged is the product of the forward delivery ratio and the reverse delivery ratio of a link. ETX is calculated using the inverse of the expected transmission probability. ETT predicts the total amount of time to send a data packet along a route, considering each link's highest-throughput transmit bit-rate and its delivery probability at that bit-rate. RoofNet's routing protocol chooses the route with the lowest ETT [4]. WCETT takes into account the interference among links that use the same channel. A discussion on link quality metrics can be found in [11], [12]. In almost all related works, a multi-hop path cost is given by the sum of the cost of each link in the path. Some authors [4], [9] state that it is better to select wireless links with significant loss rates than to favor low loss links. ReMesh initial tests used this ETX-based approach, but network performance was not satisfactory. The ReMesh real network result tests shows that the opposite choice, that is, choosing links with minimum loss rates, also leads to high throughput, with the added benefit of exhibiting more stable routes and lower packet loss rates. This is the reason why ReMesh uses the ML (Minimum Loss) metric, an ETX-based multiplicative metric.

Yarvis et al. [41] made experiences with a 100-node sensor network and DSDV (Destination-Sequenced Distance-Vector) routing protocol. The authors used a link quality metric based on the number of lost packets and discussed network performance considering packet loss rates. Like ReMesh, they suggested using the multiplying operation when calculating multi-hop route costs. However, due to limitations in the hardware platform used in the sensor network experiment, they converted link metrics to the log domain and added them to find multi-hop total costs. Besides monitoring link losses, [41] also applied passive acknowledgements in the CSMA/CA medium access control and stated that using both techniques could improve real network performance. The ReMesh project decided not to modify the medium access layer to maintain it compatible to the IEEE 802.11 standard. Even though, monitoring link losses and using multiplicative metrics were enough to improve mesh network performance in the ReMesh project.

All previously mentioned works propose the use of layer-3 routing protocols for the implementation of mesh networks. However, recent IEEE 802 efforts are focusing on the definition of a new mesh network standard based on layer-2 routing, the future 802.11s specification [1]. An implementation of the current draft has been made by the OLPC project [27] that uses layer-2 wireless mesh networks for connecting low-cost laptops in order to promote digital inclusion for children in developing countries, such as Brazil [33].

A. *Commercial vs. Community Mesh Networks*

Community wireless networks typically share a few wired Internet connections among many users spread over an urban area and do not require much coordination to deploy and operate. In contrast with commercial networks that carefully construct a multi-hop network with nodes in carefully chosen locations and uses as much as possible directional antennas aimed to engineer high-quality radio links. These networks require well-coordinated groups with technical expertise, one may result in high throughput and good connectivity.

A more ambitious vision for community networks would combine the best characteristics of both network types, operating without extensive planning, but with support of a central management, providing wide coverage and acceptable performance, consisting of the following design decisions:

1) Unconstrained node placement, rather than a topology planned for coverage or performance. The network should work well even if the topology is determined solely by where participants happen to live.
2) Omni-directional antennas, rather than directional antennas used to form particular high-quality links. Users should be able to install an antenna without knowing in advance which other nodes his antenna might talk to. Nodes should be able to route data through whatever neighbors they happen to listen;
3) Multi-hop routing, rather than single-hop base stations or access points. Multi-hop routing can improve coverage and performance despite lack of planning and lack of specifically engineered links;
4) Optimization of routing for throughput in a slowly changing network with many links of intermediate quality, rather than for route repair in a mobile network.

III. The ReMesh Project

The ReMesh project architecture for wireless mesh networks is illustrated in Figure 1.

Wireless mesh routers are installed on top of buildings or house roofs of the academic community users. Using wired Ethernet or wireless 802.11, users connect their personal workstations to their building router. Through a multi-hop wireless mesh, routers communicate to the Internet gateway(s), which is (are) installed on the top of a university building that has Internet access. The wireless gateway communicate with an authentication server, using a captive portal solution [22] in order to provide user access control to the mesh network, as it will be detailed in Section III.C.

ReMesh uses the OLSR routing protocol [8], standardized by IETF. Although it uses a pro-active link state routing algorithm, it also implements the concept of MultiPoint Relays (MPR), which is a technique to control flooding. OLSR limits the number of nodes in charge of disseminating control packets to avoid redundancies. Therefore, each node selects its MPR set, which is composed by nodes responsible for forwarding routing information from the selector node. One node fills its MPR set with the minimum number of one-hop neighbors needed to reach every two-hop neighbors. The OLSR implementation provides hop-count and ETX metric to compute the best routes. ReMesh has developed a new metric, called ML [26], which chooses routes with the minimum packet loss rates.

Besides extending the OLSR routing protocol implementation, ReMesh has also developed several network management tools, which allow monitoring network topology, network performance and wireless link quality in real-time, as described in Sections III.E and III.F. In order to provide user authentication and management services, a server is deployed as a network server.

The ReMesh wireless mesh router is a programmable device based on the OpenWRT operating system [25]. OpenWRT is a free, open-source Linux distribution that can be customized with the installation of different routing protocol implementations. OpenWRT needs 2MB of storage and runs in 125MHz processors with 16MB RAM. It can be installed in several commercial wireless routers [25]. The ReMesh project has been working with Linksys WRT54G, WRT54GS and WRT54GL 802.11g wireless routers.

For the installation of a mesh router in outdoor environments, hermetic boxes and external 18,5dbi omni-directional or 24dbi directional antennas are also used for each network node. One of the main goals in the ReMesh solution is low-cost, and it was achieved. Each mesh point costs less than US$500, compared to thousands of dollars required by commercial solutions.

The ReMesh wireless mesh network is in use since March 2006. Figure 6 shows the current outdoor network topology. It has eight fixed mesh routers and 131 registered users. According to network statistics tool, which will be presented in subsection IV-F, the ReMesh network has transferred over 700 Gigabytes of user data since March 2006.

IV. Management Issues and the ReMesh Solution

Managing WMN networks is a significantly harder task than managing wireline networks for several reasons.

One problem that arises in WMN in relation to data collection is the message overhead [7][3]. Networks that employ multiple hops using the 802.11 standard have may a limited bandwidth (whose quality can be highly variable), therefore, management messages must not consume significant amounts of this resource at any time. The first and trivial solution to extract information from network, considering that management tools are implemented at the application level, is to pool each node individually. This technique way may result in a very poor utilization of communication resources requiring a high message overhead. The level of such negative impact of management overhead is hard to predict or control, since the quality of communication links can vary so fast that even by limiting the rate and size of messages is not a reasonable approach.

The placement of a passive monitoring probe is not a trivial problem. As an example a single-hop wireless network deployed using an access point can be monitored by positioning a monitor probe element close to the access point, as it can collect network state by sniffing the traffic flowing in the wireless medium. Such technique, if applied in a multi-hop mobile network, can result in the collection of just a small part of network information, that leads to an inaccurate analysis of the network state. This is because not all communications among nodes can be heard by a probe. Consequently, monitoring multi-hop mobile networks requires a broader solution, where a greater number of nodes actively collect network state and deliver the collected information to a network manager.

Fig. 1. The ReMesh project archictecture.

A WMN have the advantage of having special kinds of node's, that forms the backhaul sector. Those nodes typically have an unrestricted power source, fixed location, generally have homogeneous hardware, offers terminal access and since they belongs to the backhaul they can monitor all the useful communication.

Monitoring tasks depend upon the temporal property of monitoring information, and such property is determined by the monitoring requirements. For example, consider a requirement such as tracking the network topology in real-time. If topology information from the network is not delivered for processing in a timely manner, the resulting view of the network can be inaccurate. On the other hand, another requirement could be to obtain a log of the statistics packets forwarded by a node without any constraints on time.

In order to accomplish the monitoring requirement, the mechanisms that implement monitoring task must address the following these challenges:

- Resource Constrained Devices; Participant devices in WMN are typically resource constrained. These devices are characterized by low processing power and limited disk space. The allocation of limited resources for monitoring can result in poor system performance.
- Almost exclusive use of wireless communication media; with few exceptions, most links are radio links, and that turns all management messages being "in-band". Therefore, management messages must not abuse on size or rate, otherwise they will negatively impact on usefulness of the network.
- Fluctuating Link Qualities; The dynamic characteristics of a wireless link, such as multi-path fading and interference from the environment, can result in widely varying in links qualities. Link quality fluctuations are likely to result in routing changes, which in turn can lead to breaks in established connections between a manager node and some managed node. This can heavily interfere with the delivery of monitoring information.
- Unfriendly Node Placement; Nodes can be installed on hard to reach places, so any direct physical interaction with a node's hardware is a difficult task that is considered an expensive and a must-to-avoid solution.

For all challenges listed above, some goals should be considered during development of management tools, as follows:

- **Low user interaction**; Tools should simplify and reduce the rate of user interaction to get some work done, but at the same time should let users change and extend all offered functionalities by editing network configuration.
- **Reliability**; Some of configuration parameters have the potential to break the access to a wireless node. One example occurs when is changing the radio channel or transmission power. Other situations where one can loosing access to a node is when changes must be done in a certain sequence. Partial execution of the changes may bring serious problems. So tools must be capable of setting up multiple parameters in one single block of commands and fall back to a failsafe mode when something goes wrong. This goal is a must because nodes can be placed at hard to reach locations, making a physical reconfiguration of a node an expensive task.
- **Low disk footprint**; Tools should depend on a minimum number of libraries or other tools and most use little space on permanent storage media. Embedded devices like nodes used on mesh backhaul have severe limited space and also a limited number of times that each storage sector can be updated without causing "burn-in" effect.
- **Low runtime footprint**; One of the main objectives of a mesh node is to allow communication between clients and the Internet, so any other task must not get in the way of this objective. This requirement forces management tools to be simple, light, capable of working in low priority, and perform only the minimum of information processing possible, such that it does not deplete main memory with management data. This goal is as strong as the economical motivation that drives cost down by simplifying the node's hardware to a bare minimum.
- **Failure resilience**; During a reconfiguration process

some nodes could be inaccessible, due to sudden interference or unstable topology. Therefor, tools should be prepared to deal with communication failures.

A. Network Initialization

In the Remesh project the first developed tool focus on installation of the operating system in the mesh node hardware and its configuration. As we use a low cost off-the-shelf hardware, developed for domestic use, its original operating system does not allow for the installation of the necessary tools for configuration as a mesh node. A substitute operating system must be loaded in the node's memory. This substitution is done by the writing of software image, that is a single file that corresponds to the entire file system. The chosen operational system is a modified version of the Linux-based OpenWRT [25].

As a first step, a new image of the system must be compiled by the tool offered by OpenWRT project, the "ImageBuilder". This image is specific to each network and to characteristics of the hardware node. A set of utility files developed by the project are annexed with the image during the compilation process. After that, this compiled image is to be recorded at the node's memory, in an inactive state and without node's identity. In order to switch the node in a capable state to form a mesh network backhaul, two new tools were developed with the goal of helping at the initial configuration task, and these tools had been annexed to the image on compilation process. These two, "Gateway node morph" and "Backhaul node morph", can execute many operations of manipulation in the files of the node, giving an identity to the node and activating the operation status.

Before the stage of compilation of the image, some mesh network common parameters are defined, as IP address of the servers and "essid" of the wireless network. The mesh node ID that identifies solely a node, in the mesh network, must be informed during the execution of these morphing tools inside of each node. These morphing tools operate in a similar form: one configures the node to function as a gateway and, the other one, as an intermediate generic backhaul node.

These morphing tools offer the quality of Low user interaction, as the common parameters of mesh network will be annexed at the software image. They require only one interaction with the user to get properly setup, since this same image will be used in all nodes. Finally only one additional parameter must be defined in each node. Therefore the node activation can be done with little work. The quality of low disk footprint is reached, because the tool had been developed with what is offered for standard in the operational system OpenWRT, namely awk, sed, cat and command shell script ash. Thus nothing was additionally installed. Morphing tools can be removed of the permanent memory after their use.

B. Network Reconfiguration

During the daily operation of the mesh network , it is common to execute some tasks in all the routers that are active, for example, to verify if certain process is in execution on each node or to modify some parameters of the network. Initially, to do such management it was necessary to access each node and by informing the IP address of each node, for then sending the desired commands.

With the purpose of automate the process the BShell (Broadcast shell) tool was developed. This tool is capable of automatically discovering the address of all nodes of backhaul in activity, open a terminal for each one and to execute the desired commands.

BShell requires only one parameter, which is the string that represents all commands that will be sent to each node forming the backhaul. Initially BShell thought a cross-layer action consults the routing table and using a filter of masks that determines the IP address of each node. For each address found, one terminal is activated and the same command string passed as parameter to the BShell and is sent to the input of the terminal. When executing tasks in each node the result on output and the integer return value are recorded at a log for future consultation.

During the development of the BShell two qualities had been prioritized: low disk footprint and failure resilience. Therefore, all utility tools used by Bshell are available as standard in the modified operational system, OpenWRT, thus no new dependency was added. The second and more important quality, failure resilience, is a must for the good functioning, therefore as the network can suffer instabilities, an error at the execution of the commands in a node must not interrupt the same process on other nodes. In case of errors, BShell should record the message or code of the error in a log and keep with it's normal functioning on the remaining nodes. Other two qualities are present: low user interaction and reliability. BShell allows that the work of executing the same sequence of commands on all nodes is made in a autonomic fashion, and thus diminishing accidental errors because of user errors. BShell is reliable and allows one exact block of commands to be executed in sequence. Even if during the processing of this block the access is cutoff, a common event when the block of commands modifies important parameters of a node's radio.

Similarly, Bcp (broadcast CoPy), is another tool developed with the sames principles of BShell, allowing the copy of files to all active nodes using the mechanism of autonomic discovery of the addresses. An interesting interaction between Bcp and BShell is when we desire to execute a very long sequence of commands that can't be passed as parameter to BShell, being the solution create a script file containing the sequence of commands, copy it to the nodes with Bcp and with BShell execute file script.

Future versions of these tools of broadcast should use internal information of OLSR [8], with the purpose to take the mechanisms of topology discovery and dissemination of the task in a more intelligent way. With the integration with the OLSR it will be possible to discover the list of the nodes that belong the network not only at the moment when routing table was consulted, but for a wider period of time.

Another possible improvement is the creation of spontaneous clusters, generated with the purpose of helping the

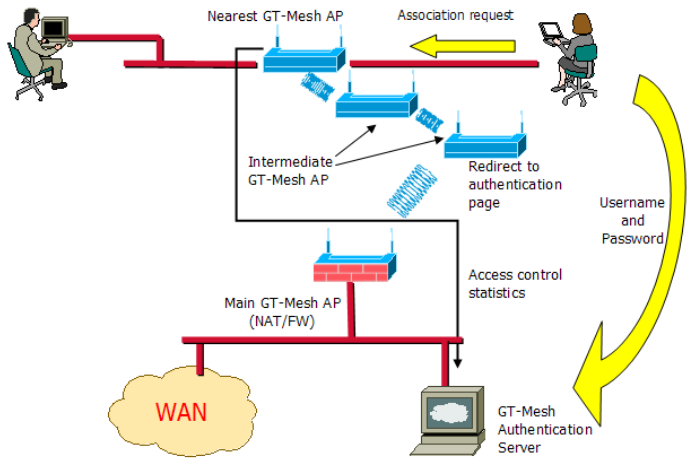

Fig. 2. Clients authentication process.

dissemination of files or commands. Currently only one node possesses the tools BShell and Bcp. This node is called manager node, and, as manager, it possesses the responsibility of creating individual connections to each one of the other nodes of the mesh network, and through these connections carry the tasks sequentially. The idea is to create clusters to dilute the responsibility of the manager node, spreading the tasks to several others nodes. With the additional information that can be extracted of the routing protocol is possible to discover how many and which are the neighbors of each node. With these information clusters can be formed by sectors of nodes where the node with the highest number of neighbors would be elected as a master node of a cluster. It is his responsibility to spread the task to its neighbors and to inform the result to the manager node. While the manager node would only need to spread the tasks to each master node of each cluster.

C. User Authentication and Access control

User authentication service, access control and statistics data from user access of the ReMesh network are provided by WifiDog software[22]. The WifiDog software is a captive portal solution, licensed under the CC-GNU GPL (Creative Commons GNU General Public License), and is designed with many others features, like centralized access control, full bandwidth accounting among others. A captive portal comprehends the conjunction of a dynamic firewall and a web page, in which all traffic is blocked, except the HTTP traffic that is redirected, until the user completes the authentication process. The authentication process requires a login page, so all HTTP traffic of each client is redirected, regardless of address or port, to a special page hosted in the authentication server. This page sends a HTTP response which orders the users browser to make a new request to the login page. The authentication server then checks the user name and the password against a database and, if correct, reconfigures the firewall. Figure 2 shows clients authentication process.

The ReMesh network must provide Internet access for both wired and wireless clients. Unfortunately, the WifiDog solution is not able to authenticate two different input interfaces, one for the wired clients (APs Ethernet interface) and other for the wireless clients (APs IEEE 802.11 interface). Because of this limitation, there are two different approaches for the authentication process. The wired clients authentication process is done by the ReMesh node which the client is connected to. The node filters forwarding traffic from the Ethernet interface to the backhaul wireless interface with the original WifiDog configuration. The wireless clients authentication is supported only by the main ReMesh node, which act as an Internet gateway for the rest of network, filtering forwarded traffic from the wireless interface to the Ethernet interface with a modified version of the WifiDog software. This solution makes sure that all traffic from clients will be filtered.

Some issues appeared on prototype stage of ReMesh network that forced a special treatment of wireless clients. All of them are related to the potencial mobility of wireless clients. As a client moves between coverage areas from different ReMesh routers, it keeps the authentication valid because his traffic is still being filtered by the Internet gateway. If a wireless client were authenticated by the mesh node they are connected to, once move to another mesh node coverage area it would have to authenticate itself again.

Another problem with the WifiDog solution is related to the fact that the original developers considered only the cenario of single hop wireless networks. Some extra security measures, only applicable to this type of network, were used, such as the source MAC filtering of authenticated users. This approch in a Multi-hop network is not possible because the source MAC of a frame received by the gateway is rarely the users MAC interface. The source MAC from a frame is usually the address from the last hop node from mesh's backhaul.

Only nodes morphed to gateway node by initial configuration tool executes NAT (Network Address Translation) and firewall functions. Figure 3 shows this architecture.

On server side of WifiDog is the PHP module. It is structured in dynamic pages hosted in the authentication server. These dynamic pages are responsible for user authentication, user and node (AP) management, accounting information, etc. In ReMesh project, these dynamic pages were customized as follows:

- Only administrator can manage user accounts;
- Different users cannot use the same login name;
- Some statistics data (online users, bandwidth consumers, individual user reports, top 10 most frequent users etc) are available for every one; and
- Source MAC filtering on frames of wireless authenticated users was disabled.

D. Network Topology View

One of the most useful and needed capabilities of a network management system is to present the topology of the network. In networks which rely on a wireline infrastructure, this is a very simple task because changes to the topology are very

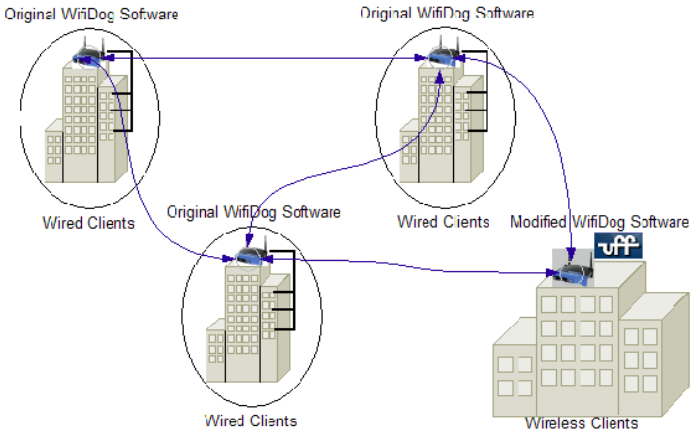

Fig. 3. ReMesh WifiDog installation.

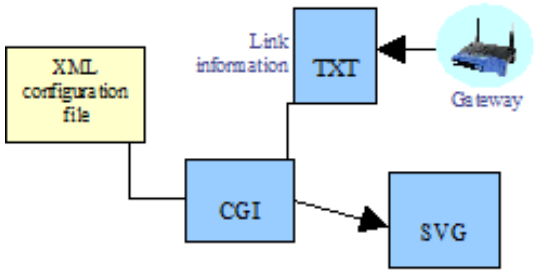

Fig. 4. Topology visualization tool operation.

```
<topologia src="topologia3.jpg" width="800" height="600" gateway="200.20.15.238">
   <legenda src="legenda.jpg" x="600" y="480" width="200" height="120"/>
   <roteador id="rot1" x="370" y="214" ip="10.0.0.1" href="http://mesh.ic.uff.br"/>
   <roteador id="rot2" x="385" y="273" ip="10.0.0.2" href=" http://mesh.ic.uff.br"/>
   <roteador id="rot3" x="490" y="300" ip="10.0.0.3" href=" http://mesh.ic.uff.br"/>
   <roteador id="rot4" x="360" y="346" ip="10.0.0.4" href=" http://mesh.ic.uff.br"/>
   <roteador id="rot5" x="386" y="373" ip="10.0.0.5" href=" http://mesh.ic.uff.br"/>
</topologia>
```

Fig. 5. Topology configuration file example.

infrequent. In mesh networks, on the other hand, the characteristics of the topology changes very frequently due to the the volatile environment. Thus, the management station needs to collect connectivity information from nodes, forming the backhaul of network very often. An implication of this is the increased message overhead to collect topology information.

Because of characteristics of wireless environments, signal quality can vary quite dramatically. Thus, fading and jamming may result in a link going down periodically. An effect of this is that the network topology from a graph theoretic point-of-view changes.

Moreover, in order to make the network administration and maintenance task easier, a mesh topology visualization tool should show link quality metric values, so the administrator can monitor the quality of each link and identify issues. As another feature, a topology visualization tool can provide configuration or traffic information for each mesh node, integrating other management tools into one.

The first tool used on ReMesh project was the “dot draw” plugin of the OLSR distribution, which generates a simple graph representing nodes and its links with their metric. It was hard to visually understand the presented data (e.g. neighborhood, route to the Internet gateway and spatial localization of a node), because graph presentation is build to get a better distribution of graph elements, not considering their geographical location.

The ReMesh project developed a new graphic tool for visualizing mesh network topologies prioritizing geographical meaning. The tool uses the SVG (Scalable Vector Graphics) web standard, which is based on XML, to build an interactive network map, drawing the graph on top of an image that represents the network geographical placement, like a map or a satellite photograph. As ReMesh uses the ML metric, link quality is represented by a color scale defined according to its ML value. The visualization tool is available for standard web browsers.

This new tool gives the human manager the capacity to quickly identify possible sources of problems when users complain about the quality of their Internet connection. A simple visual inspection of the network map can bring to light some ideas, e.g. neighborhood suffering of a heavy interference if the users node are surrounded by red links or an energy problem if a node disappeared from map.

Basically, the tool is a CGI program that runs in a web server. It uses a XML-based topology configuration file as an argument and generates SVG code. The CGI program and topology configuration files must be in the same folder. The CGI program dynamically gets link quality information from mesh neighbor routers and their IP addresses from a text file, which is generated by the OLSR routing protocol and stored in the gateway router. Figure 4 shows the operation of the topology visualization tool.

The XML-based topology configuration file allows customization of the network map according to specific mesh network information. It provides the background image URL, gateway IP address and picture screen size, the subtitle picture URL explaining how map link colors are related to link quality metric values and identification (id), position and IP addresses for each fixed mesh router. Additionally, the topology configuration file permits specifying a URL for each router, which can indicate a customized web page giving direct access to router configuration or traffic information. In our implementation, it points to the MRTG tool web page for each router. Figure 5 shows an example of the XML-based topology configuration file, showing the X and Y position of each node, forming the mesh backhaul, in the image “topologia3.jpg”

E. Network Performance Monitoring

As networks grow bigger and more complex, the need for informative and easy-to-use network management tools is now greater than ever. These tools are used both to monitor network devices, and most of them use some sort of web-interface for cross platform operation. The following two tools

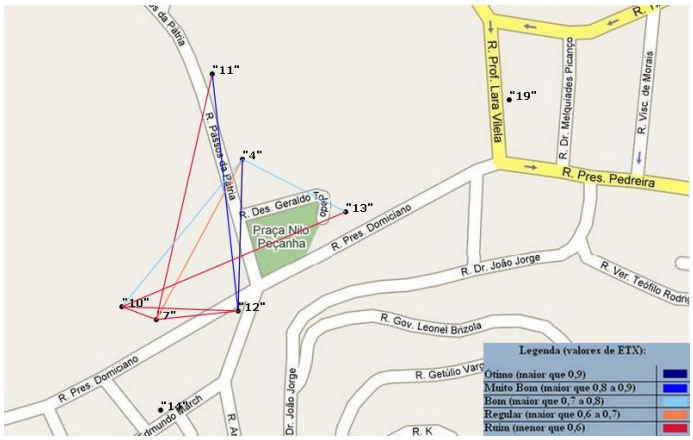

Fig. 6. illustrates the ReMesh network topology generated by the graphic visualization tool.

will be briefly presented; MRTG (the Multi Router Traffic Grapher)[14], and Ntop[10]. The first tool uses SNMP to poll information from routers, whereas the latter is a web-based tool for measuring numerous attributes of network.

MRTG[14] is probably the most widely deployed network monitoring suite on the Internet. The authors have this to say about MRTG: "The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing graphical images which provide a live visual representation of this traffic. MRTG is based on Perl and C and works under UNIX and Windows NT. MRTG is being successfully used on many sites around the net."

Ntop[10] is a Web-based traffic measurement and monitoring application that has the ability to monitor and manage a network from a remote location without the need to run specific client applications to analyze traffic information, has a minimal requirements and can be extended via dynamically loadable software components by users. NTop focus on Traffic measurement, characterization and monitoring, detection of network security violations and informations for network optimization and planning

Above tools are widely used in the Remesh project.

F. Network Statistics

To obtain statistics from the mesh network, the ReMesh solution proposes an alternative approach to the use of the Simple Network Management Protocol (SNMP) [6]. Although SNMP has become a solid standard, it has presented some drawbacks to the project.

The first is related to the specific characteristics of wireless mesh networks: SNMP standard is not able to retrieve all the relevant information on this kind of network. Interesting statistics such as currently used gateway or number of hops to it, which are both relevant in mesh networks, cannot be obtained through SNMP. Another example of this limitation is the information about bandwidth. SNMP is only able to retrieve data about the currently used bandwidth. This may be enough for estimating a link usage in a wired network. However, in wireless networks the capacity of the links vary over time, making it impossible to determine if a low report of a link used bandwidth is caused by low traffic or by problems in the communication. In other words, the available bandwidth is an extremely important parameter.

A second issue is related to the large amounts of resources consumed by the SNMP protocol implementation. Using the implementation provided by OpenWrt, the SNMP daemon consumes more than 10% of the memory available in the hardware. That is more than two times the amount of memory consumed by the OLSR routing protocol daemon (around 4.9%). Given the limited amount of avaliable memory in this kind of device, resource consuption becomes a real constraint.

Considering these two factors, the ReMesh solution implements a different system. This proposal is divided in three modules: a shell script used to obtain the statistics, a database to store the collected data and a web page to exhibit the information.

The first module is executed in the network routers. Since it is a script, it can obtain any information available to an user through a Linux shell. Once every ten minutes, this module collects the statistics and passes them to the database using a HTTP request to a CGI in a web server. The collected information is used as a parameter for the CGI, which parses the arguments and stores the data in the database.

A web page is available to display the stored information in the form of graphs. Currently, there are twelve available router statistics: network delay, available bandwidth, packet loss and number of hops (all related to the currently used gateway), CPU usage, number of active processes, free and used memory, in bytes and out bytes for the wireless and LAN interfaces. The user is able to choose up to two statistics at a time well as the considered time period and the set of considered nodes. There is also information about online users, such as transferred bytes and IP addresses. Figure 7 shows network delay and available bandwidth graphs generated by the proposed solution.

It is important to note that network delay, available bandwidth and packet loss are obtained through active measurements, using the well-known tools *ping* and *iperf* during a short period. With this approach, it is possible to obtain real statistics about available resources in the network. On the other hand, this active monitoring technique interferes with the clients communications. However, since the duration of the probe is small, the negative impacts are reduced.

Some additional statistical data are collected by Captive portal, includes:

- Ten highest bandwidth (Figure 8), frequent and mobile users;
- Number of new connections per hour of the day (Figure 10);
- Number of individual user visits per weekday(Figure 9) and per month.

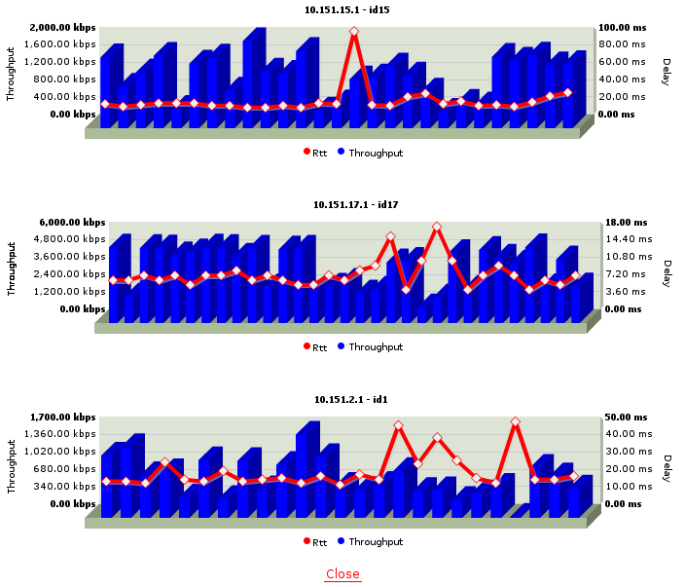

Fig. 7. Example of graphs generated by the proposed tool.

User (username)	Incoming	Outgoing	Total
pascoal	163,6G	207,1G	370,7G
jviana	76,5G	128,7G	205,3G
fidi	58G	50,7G	108,8G
wgramacho	26G	5,4G	31,4G
dvianna	18,9G	3,1G	22G
rtoso	18,5G	879,1M	19,4G
rcapua	12,3G	1,3G	13,5G
alvaro	8,8G	1,2G	10G
luciana	881M	4,4G	5,2G
ilima	4,1G	819,5M	4,9G

Fig. 8. 10 highest bandwidth consumers from outdoor network.

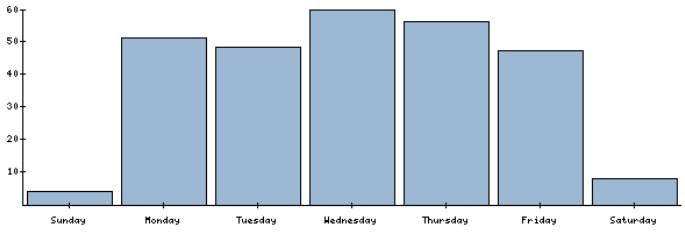

Fig. 9. Number of individual user visits per weekday.

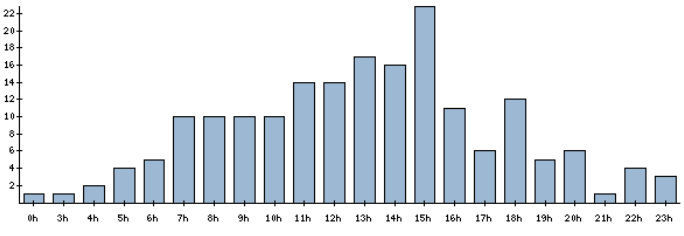

Fig. 10. Number of new connections opening per hour of the day.

V. Open Issues

Either some issues found by ReMesh project remain open because they could be initially handled by a workaround or they could be safely ignored. As the network initially had a small scale some issues did not pose a dangerous threat.

However, as ReMesh project grows in network size and scale, some left behind open issues came across, getting in the way of network evolution. As a recent experience of project members on working with routing issues, the cross-layer technique proved to be an interesting source of solution. The cross-layer technique is based on inter-layer information exchange across the traditional layers of the protocol stack. Initially protocol stack was built using layers to allow better separation of concerns and make possible to exchange the implementation of a layer without interfering with others, by making each layer independent from above layers. Although that helped at the beginning of Internet by making it simpler to develop an issue [17] on todays level of development, because some lost knowledge hidden in lower layer avoids the use of smarter and more complex techniques that may improve network performance.

A. Dynamic Channel

As the popularity increase of consumer wireless network products that implements 802.11b/g standards, the only three channels, that do not suffer interference on each other (channels three, six and eleven) are utilized even more.

To address that problem, the selection of the channel used by single radio mesh networks should be the single channel that have the lowest interference on the entire network.

Currently the selection of channel happen at the deployment time of the first pair of nodes, so the channel chosen is the best one only on that specific time. As time passes and as the mesh network grows another channel could become a better one, thus the challenge is to build a mechanism of an autonomous technique of dynamic channel selection that will keep in constant evaluation on all channels [19]. Such technique consists the tracking the channel state of each neighbor of every node forming the network backhaul and apply the acquired knowledge choose the channel that will maximize the performance of whole network.

One possible criteria is to assign a value on each channel that reflects the observed noise on each node. So as free the channel is on a neighbor of a backhaul node the greater it's value, however observation made on most used nodes during a long window of time will give a value with a bigger weight. Another way, channel with more noise will receive a negative value and if such channel could provoke a network partition a bigger negative value will be assigned to it.

Special care should be taken to avoid unstable channel assignment, as each change, if not taken with good synchronization, can create partition on the network. But even when changes complete successfully dynamic channel changes can cause high packet losses.

B. Dual Frequency

When multi-hop ad-hoc networks use the 802.11 standard in a single radio setup, they have serious problems [40]. Those problems have great impact on capacity of the network to exploit the maximum potential of each link. They are caused by, among others the shared communication media and half-duplex radios. The events of message collisions are on type of those problems that are very common, so common they severely impact on the maximum rate of goodput. This rate that degrade very fast on each new hop, in this way limiting the range where mesh network can offer an useful coverage.

One possible way to address this issue, that's gets worse as network grows and its utilization level, but keep using relatively simple and cheap radios equipments thats implement 802.11 and allowing greater use of broad coverage of multi-hop setup, is the use of more radio interfaces [20], [32], operating on non self-interfering channels. As a benefit each node will be able to receive and transmit messages on different channel at the same time and because of that greatly improving scalability on the use of multi-hops. Another benefit is the potential of lowering interferences and collisions among neighbors transition by reducing the use intensity of each channel, because will be less neighbors working on the same channel.

The challenge of making a good use of multiples radio interfaces on diverse channels is to create the channel a selection technique that uses diversity as an advantage. At least three types of techniques can be easily raised, the first one is static that in an event of reconfiguration will analyze network status, select best channel for each link and reconfigure radios based on that selection [32]. These channel will remain the same until next reconfiguration event occurs. The second one is dynamic, which do the same processing as the first, but it keeps in a continuous loop choosing the best channel and doing the reconfiguration, trying to maintain the network on continuous optimum state even with environment changes. Third and last one is a hybrid technique that blends the best characteristics of the other two, where at least one interface will use static adaptation to improve stability and connectivity, even if its means using a channel that in some sector of network is a noisy one , and the rest of radio interfaces use a dynamic to improve performance on changing environment conditions.

The same care taken in dynamic transition power selection is also necessary to avoid an instability strong enough to compromise network capacity or the worst, when a partition of the topology happens.

C. Dynamic Transmission Power

One of parameters that have an important impact on how radio works and their performance is the transmission power. The higher is the power output, the broader and longer the covered area by the network radio's signal, and beyond that, it has a positive effect on maximum sustained throughput of a link. However higher the output also increases interference on neighbors, and this issue can lead to decrease of performance observed on the network as a whole.

Currently this parameter, power level, is adjusted on a manual fashion, by some empirical knowledge of local and briefly tests, or by simply adjusting on the maximum safe level.

One possible way of correcting this naive strategy, transforming it in a smarter transmission power adjustment technique [31], [13], is to use a cross-layer technique. In this case use additional information available on routing layer, since the routing protocol used on ReMesh project,OLSR [8], is a link-state protocol it not only knows the links to direct neighbors but have a global view of all network links. Such technique would try to maximize the quality of link's to MPRs and do the opposite to the others nodes. These two objectives can be contradictory between them, because the first one tries to increase the power level to improve link quality and the second one tries to decrease it in an attempt to minimize induced noise on neighbors.

The reason that explains the difference between these two objectives, the first one prioritizing links to MPR come by the fact that these links can be candidates for forwarding messages to Internet, as the others links, if used, will be on following hops. So decrease the interference on links that are candidates for later forwarding is desirable. This decrease is even more desirable if the time needed to recover on message loss is considered, because if the messages loss is long enough the recovery mechanism of layer-2 fails, forcing the upper layer-3 to recover using slower end-to-end techniques.

Some precautions should be taken because too much reduction on power level could harm the ability of routing protocol to discover the real topology, thus decreasing the number of useful links. The level of adjustment on power level should maximize a utility function that takes account the local gain of one hop neighbors on MPR with loses of global performance provoked by interference on neighbors aways with two or more hops.

Beyond the use of utility function to control the adjustment of power level, other issues can have an important influence, in e.g. the event of transmission of especial control messages of the routing protocol by a node to the rest of network , which are fundamental for discovery and maintenance of network's topology, can force the usage of a higher power level. Another influent event is when topology had suffered some severe change, as a loss of a node or a network partition, could use increased level of transmission power to correct or soften the negative effect of such event.

D. Autonomous Network Configuration

As the mesh network grows in size, various tasks that initially were easily carried on a manual fashion turn to be the source of a high volume of undesirable work to be handled by a human manager. As the technology evolves and conquer new frontiers, the number of available human resources with high level of proficiency become heavily limited, increasing the pressure for the development of simpler, autonomous and broader management and configuration tools.

Presently, each mesh node needs to incur a setup process individually by a user, and that user needs to have good knowledge of wireless network and of some very specific issues of mesh networks. Each operation parameter, like essid, radio channel and node identification are setup before their deployment. It would be better if the setup process could be done after the deployment of a node, and even then with no or little user interaction, removing from the user the obligation of domination of all aspects of mesh networks so the mesh would be autonomously configured when new nodes join the network.

The mechanism that gives a mesh network this autonomous capacity should be able to manipulate every work parameter in an adequate way from any functional state, which includes the initial state, where node will turn on for the first time, or a state in which the node was reallocated from one sector of the network to another one without any previous measure to prepare the management mechanisms for that reallocation. A couple of goals should be matched. Security functionalities that prevents a node from operating on a wrong network, offer resistance against DoS (Denial of Service) attacks or accept commands from unauthorized entities. Others goals include the needed time for a reconfiguration to be less that the time users are willing to wait and during the period when no reconfiguration is asked or needed this mechanism should not cause a disturbing overhead on network performance.

Every component of the implementation of this mechanism should serve as an infrastructure to other tools that should be developed to complement the network management with additional behavior, like dynamic transmission power or channel selection. Doing so the implementation of these other tools would be simplified and made easier to implement novel improvement techniques. Integration between tools should be done with the usage of well defined interfaces and simple access methods, that have minimum impact on implementation and should be powerful enough to allow adequate information exchange.

E. Integration of management tools

With development of various tools, each one focusing on a restricted set of problems, the task of network management became a work of collecting disperse data and giving a unified meaning. A new and more centralized way should be developed that offers one or a few tools that give a view of network state, overloaded with information collected by numerous different tools, treated, filtered and combined in a such unified view. This way, management systems can accelerate the time needed by a human manager to detect problems and its sources.

Following the example of other solutions [24], [29], the topology visualization tool can be a good place to aggregate data of others tools as shown in Figure 11, because it is as naturally organized as the geographical displacement of nodes. Thus, the topology tool can combine information of the network to offer a richer map to a network manager, allowing him to quickly access all broader data about network. For instance, the quality of all links or the number of authenticated users on each node, and with a simple request the manager could receive more detailed data on specific nodes, such as the names of authenticated users, performance metrics like memory consumption or recent activity history.

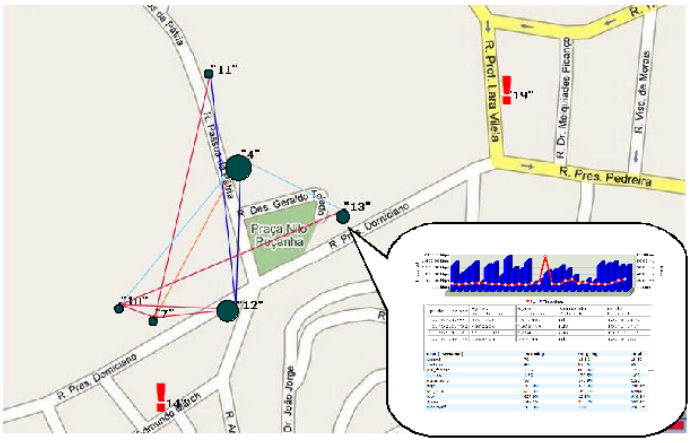

Fig. 11. Preview of topology tool with integrated data.

The ultimate objective of integrating management tools is to pave a new way for a network manager to gather needed network information in a faster and easier way than before with a disperse set of tools. Such integration should let a manager decide on how deep or which layer data is to be displayed, to avoid unneeded overwhelming flooding of information.

VI. Concluding Remarks

This work addressed a number of management issues and outlined the solutions adopted by the ReMesh project. Specifically this work presented the following tools:

- **Gateway node morph**: Mesh node initialization as an Internet gateway;
- **Backhaul node morph**: Mesh node initialization as backhaul node;
- **BShell** and **Bcp**: Mesh node reconfiguration through autonomic commands;
- **WifiDog**: Mesh user authentication and access control;
- **SVG**: Mesh network topology view; and
- Mesh performance measurements and statistics.

Furthermore, this work raised and discussed a number of open management issues in wireless mesh networks, including the use of dynamic frequency selection, the use of dual frequencies, dynamic transmission power, autonomous network configuration and the integration of management tools. Managing large and unplanned wireless mesh networks has many challenges and the authors encourage the community to start addressing them, not only from a theoretical point of view, but also from a practical one, considering realistic channels and devices.

REFERENCES

[1] IEEE P802.11s/D0.02, Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking. June 2006.

[2] Ian F. Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks: a survey. *Comput. Netw. ISDN Syst.*, 47(4):445–487, 2005.

[3] Remi Badonnel, Radu State, and Olivier Festor. Management of mobile ad hoc networks: information model and probe-based architecture. *Int. J. Netw. Manag.*, 15(5):335–347, 2005.

[4] John Bicket, Daniel Aguayo, Sanjit Biswas, and Robert Morris. Architecture and evaluation of an unplanned 802.11b mesh network. In *MobiCom '05: Proceedings of the 11th annual international conference on Mobile computing and networking*, pages 31–42, 2005.

[5] Raffaele Bruno, Marco Conti, and Enrico Gregori. Mesh networks: Commodity multihop ad hoc networks. *IEEE Communications Magazine*, pages 123–131, 2005.

[6] J. D. Case, M. Fedor, M. L. Schoffstall, and J. Davin. Simple network management protocol (SNMP). RFC Experimental 1157, Internet Engineering Task Force, May 1990.

[7] Wenli Chen, Nitin Jain, and Suresh Singh. ANMP: Ad hoc network network management protocol. *IEEE Journal on Selected Areas in Communications*, 17(8):1506–1531, 1999.

[8] T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR). RFC Experimental 3626, Internet Engineering Task Force, October 2003.

[9] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In *MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 134–146, New York, NY, USA, 2003. ACM Press.

[10] L. Deri and S. Suin. Effective traffic measurement using ntop. *Communications Magazine*, 38(5):138–143, may 2000.

[11] Richard Draves, Jitendra Padhye, and Brian Zill. Comparison of routing metrics for static multi-hop wireless networks. In *ACM SIGCOMM*, 2004.

[12] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128, New York, NY, USA, 2004. ACM Press.

[13] Tamer A. ElBatt, Srikanth V. Krishnamurthy, Dennis Connors, and Son K. Dao. Power management for throughput enhancement in wireless ad-hoc networks. In *ICC (3)*, pages 1506–1513, 2000.

[14] MRTG (Multi Router Traffic Grapher). http://oss.oetiker.ch/mrtg/. Accessed in 3/July/2007.

[15] W. G. Griswold, P. Shanahan, S. W. Brown, R. Boyer, M. Ratto, R. B. Shapiro, and T. M. Truong. Activecampus - experiments in community-oriented ubiquitous computing. *IEEE Computer*, 2004.

[16] C. Ho, K. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer. A scalable framework for wireless network monitoring. In *ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, September 2004.

[17] Z Wang D Sirovica I Wakeman, J Crowcroft. Layering considered harmful. In *IEEE Network*, pages 20–24, January 1992.

[18] David B. Johnson, David A. Maltz, and Josh Broch. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks. pages 139–172, 2001.

[19] Chuang Justin and Sollenberger Nelson. Performance of autonomous dynamic channel assignment and power control for tdma/fdma wireless access. *IEEE J SEL AREAS COMMUN*, 12(8):1314–1323, 1994.

[20] P. Kyasanur and N.H. Vaidya. Routing and interface assignment in multi-channel multi-interface wireless networks. In *Wireless Communications and Networking Conference*, volume 4, pages 2051– 2056, March 2005.

[21] Allan Leinwand and Karen Fang Conroy. *Network management (2nd ed.): a practical perspective*. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1996.

[22] Michael Lenczner. Wireless portals with wifidog. *Linux J.*, 2005(140):8, 2005.

[23] S. Hailes M. Lad, S. Bhatti and P. Kirstein. Enabling coalition-based community networking. In *The London Communications Symposium (LCS)*, September 2005.

[24] Meraki. http://meraki.com/. Accessed in 5/July/2007.

[25] OpenWrt. http://openwrt.org. Acessed in 03-2007.

[26] D. Passos, D. Teixeira, D.C. Muchaluat-Saade, L.C. Schara Magalhes, and C. Albuquerque. Mesh network performance measurements. In *5th International Information and Telecommunicatios Technologies Symposium*, December 2006.

[27] OLPC (One Laptop per Child). http://laptop.org. Accessed in March/2007.

[28] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir R. Das. Ad hoc on-demand distance vector (AODV) routing. RFC Experimental 3561, Internet Engineering Task Force, July 2003.

[29] Netequality project. http://www.netequality.com/. Accessed in 5/July/2007.

[30] K.N. Ramachandran, E.M. Belding-Royer, and K.C. Almeroth. Damon: a distributed architecture for monitoring multi-hop mobile networks. In *IEEE International Conference on Sensor and Ad hoc Communications and Networks*, October 2004.

[31] Ram Ramanathan and Regina Hain. Topology control of multihop wireless networks using transmit power adjustment. In *INFOCOM (2)*, pages 404–413, 2000.

[32] Ashish Raniwala, Kartik Gopalan, and Tzi cker Chiueh. Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 8(2):50–65, 2004.

[33] Luiz Claudio Schara Magalhes Ricardo Campanha Carrano, Michail Bletsas. Mesh networks for digital inclusion - testing olpc's xo mesh implementation. In *8o Forum Internacional de Software Livre*, 2007.

[34] S. Roch. Nortel's wireless mesh network solution: Pushing the boundaries of traditional WLAN technology. *Nortel Technical Journal*, October 2005. Available at http://www.nortel.com/solutions/ntj/collateral/ntj2_wireless_mesh.pdf.

[35] C. Santivanez, B. McDonald, I. Stavrakakis, and R. Ramanathan. On the scalability of ad hoc routing protocols. In *IEEE INFOCOM*, 2002.

[36] C. Santivanez and R. Ramanathan. Hazy sighted link state (HSLS) routing: A scalable link state algorihm, March 2003. In BBN Technical Memorandum, No. 1301.

[37] Cisco Wireless Mesh Networking Solution. http://www.cisco.com/go/wirelessmesh. Accessed on July/2007.

[38] N. Tsarmpopoulos, I. Kalavros, and S. Lalis. A low-cost and simple-to-deploy peer-to-peer wireless network based on open source linux routers. In *International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities (TRIDENTCOM'05)*, pages 92–97. IEEE Computer Society, 2005.

[39] S. Weber, V. Cahill, S. Clarke, and M. Haahr. Wireless ad hoc network for dublin: A large-scale ad hoc network test-bed. *ERCIM News*, 2003.

[40] S. Xu and T. Saadawi. Does the ieee 802.11 mac protocol work well in multihop wireless ad hoc networks? 39:130–137, Jun 2001.

[41] M.D. Yarvis, W.S. Conner, L. Krishnamurthy, J. Chhabra, B. Elliott, and A. Mainwaring. Real-world experiences with an interactive ad hoc sensor network. In *ICPPW*, 2002.