Emerging Wireless Networks for Social Applications

Raúl Aquino Santos[1], Luis A. Villaseñor González[2], Víctor Rangel Licea[3], Miguel A. Garcia-Ruiz[1], Arthur Edwards Block[1]
[1]Faculty of Telematics, University of Colima, Av. Universidad 333, C. P. 28045, Colima, Colima, México.
[2]CICESE, Research Centre, carr. Tijuana-Ensenada, km. 113, Ensenada, B.C. Mexico
[3]Department of Telecommunications, National Autonomous University of México, Mexico, D.F.

ABSTRACT

This chapter describes the implementation and performance evaluation of a novel routing protocol called Pandora, which is designed for social applications. This protocol can be implemented in a broad number of devices, such as commercial wireless routers and laptops. It also provides a robust backbone integrating and sharing data, voice and video between computers and mobile devices. Pandora offers great performance with both fixed and mobile devices and includes important features such as: geographic positioning, residual battery energy monitoring, and bandwidth utilization. In addition, Pandora also considers the number of devices attached to the network. Pandora is experimentally evaluated in a testbed with laptops for the first stage and commercial wireless routers for the second stage. The main goal of Pandora is to provide a reliable backbone for social applications requiring a quality of service (QoS) guarantee. With this in mind, the following evaluation of Pandora considers the following types of traffic sources: transport control protocol (TCP), voice, video and user datagram protocol (UDP) without marks. Pandora is also compared with different queuing disciplines, including: priority queuing discipline (PRIO), hierarchical token bucket (HTB) and DSMARK. Finally, an Internet radio transmission is employed to test the network re-configurability. Results show that queuing the PRIO and HTB disciplines, which prioritizes UDP traffic, performed the best.

Keywords: Emerging networks for social applications, hybrid wireless mesh network, Pandora protocol, wireless ad hoc networks, and routing algorithms.

.

INTRODUCTION

Humans have always suffered from the effects of natural catastrophes, including earthquakes, hurricanes, floods, volcanic activity, tornados, droughts, tsunamis and famine. Presently, there are several proposals to better meet the special demands placed upon computer communications and information infrastructure in emergency and rural wireless networks for social applications. The need to provide immediate communications through an infrastructureless computer network that is connected to the Internet in emergency situations is critical in emergency response and disaster recovery (Portmann, 2008). Consequently, there are presently several interesting proposals to deal with the extremely important objective of better managing emergencies.

The use of emerging wireless networks for emergency and rural communities has received increased attention from both research and industry. When traditional communication and electrical infrastructure fails because of natural disasters or other unforeseen causes, a temporary and reliable back-up system must provide for the efficient capture and local transference of emergency information.

The opportune and accurate broadcast of information during disasters is a vital component of any disaster response program designed to save lives and coordinate relief agencies. In moments of disaster, when conventional systems are down, wireless broadband communications networks can provide access to databases that provide data, audio, video or geographical information essential to provide emergency assistance.

Emergency and rural wireless networks need to include fault tolerance (robustness), provide low cost voice/video communication, and possess different architectures that are easy to set up (e.g. ad hoc mode). Furthermore, they should also be flexible to provide interoperability among different wireless technologies, including existing operating systems, plug-and-play functionalities, and proactive and reactive algorithms.

Some reasons for the success behind hybrid wireless mesh network (HWMN) technology include: 1) they provide very inexpensive network infrastructure due to the proliferation of IEEE 802.11 based devices, 2) they offer easy network deployment and reconfiguration, 3) they give broadband data, audio, and video support, and 4) they use the unlicensed spectrum (Braunstein, et al, 2006). Because of these advantages, HWMNs find many applications in a variety of situations ranging from fixed residential broadband networking, based on rooftop wireless mesh networks, to emergency response networks for handling large- scale disasters.

This work analyzes the feasibility of voice over internet protocol (VoIP) in a HWMN for emergency and rural communications over the Pandora protocol. The proposed network architecture is composed of two distinct layers:
(1) An ad hoc network which is composed of wireless mesh clients (WMCs) and (2) wireless mesh routers (WMRs), with a backbone connection between the WMRs (Portmann, 2008). In this architecture, the two types of nodes that comprise the wireless mesh network (WMN) suffer different constraints. WMCs located at the end points have limited power resources and may be mobile, while WMRs possess minimum mobility but do not suffer from power constraints.

VoIP applications must take into account QoS parameters such as bandwidth, jitter, latency and packet loss. Consequently, Pandora should be compared with the PRIO, HTB, and DSMARK queuing disciplines using different kinds of traffic sources, including TCP, voice, video and UDP without marks.

STATE OF THE ART OF ROUTING ALGORITHMS FOR WIRELESS MESH NETWORKS

An infrastructure for social networks can be easy deployed using wireless mesh technologies. However, the heart of such wireless mesh technologies is their routing algorithms. Several wireless mesh routing protocols have been reported in the literature. The mobile mesh border discovery protocol (MMBDP), which is a robust, scalable, and efficient mobile ad hoc routing protocol based on the "link state" approach is presented in (Grace, 2000). A node periodically broadcasts its own link state packet (LSP) on each interface participating in the protocol. LSPs are relayed by nodes, thus allowing each node to have full topology information for the entire ad hoc network. From its topology database, a node is able to compute least cost unicast routes to all other nodes in the mobile ad hoc network.

The topology dissemination based on reverse-path forwarding (TBRPF) protocol, which is a proactive and link-state routing protocol designed for mobile ad hoc networks, is described by (Ogier, et al, 2004). TBRPF provides hop-by-hop routing along the shortest path to each destination. Each node running TBRPF computes a source tree, based on partial topology information stored in its topology table, using a modification of Dijkstra´s algorithm. To minimize overhead, each node reports only part of its source tree to neighbors. TBRPF uses a combination of periodic and differential updates to keep all neighbors informed of the reported part of its source tree. Each node also has the option of reporting additional topology information to provide improved robustness in highly mobile networks.

A well known ad hoc routing algorithm and variant of ad hoc on-demand distance vector (AODV) is described in (Pirzada, et al, 2006). Ad hoc on-demand multi-path distance vector (AOMDV) provides loop-free and disjoint alternate paths. During route discovery, the source node broadcasts a Route_Request packet that is flooded throughout the network. In contrast to AODV, each recipient node creates multiple reverse routes while processing the Route_Request packets that are received from multiple neighbors. Dynamic source routing multi-path (DSR-MP) is also described in (Pirzada, et al, 2006). In the multi-path version of the DSR protocol, each Route_Request packet received by the destination is responded to with an independent Route_Reply packet.

The ad-hoc on-demand distance vector hybrid mesh (AODV-HM) protocol is analyzed in (Pirzada, et al, 2007). The aim of AODV-HM is to maximize the involvement of mesh routers in the routing process without significantly lengthening the paths. In addition, the author's objective is to maximize channel diversity in the selected path. To implement these features, they make two changes to the Route_Request header. First, they add a 4-bit counter (MR-Count) to indicate the number of mesh routers encountered on the path taken by the Route_Request. They further add a 7-bit field (Rec-Chan) to advertise the optimal channel to be used for the reverse route.

The weakness of the previous mesh routing protocols considered in this study is that they are measured in terms of the number of hops or the shortest path. However, these parameters are not always the most adequate when dealing with wireless mesh networks, primarily because of the dynamic characteristics of their links. Another important concern is that the previously mentioned protocols are adaptations of protocols for wireless ad hoc networks, meaning that they are not specifically developed for wireless mesh networks.

WIRELESS MESH NETWORK TESTBEDS

Recently, a number of testbeds have been deployed by the research community, moving the focus of research activities to real implementations. Nevertheless, only limited research has encompassed a global approach that tackles the two main tasks of a WMN: the self-organization of the mesh backbone and the seamless connectivity for end-users.

The design and implementation of self-configuring, secure infrastructure mesh network architecture, called MeshCluster, which uses multi-radio network nodes, is presented in (Ramachandran, 2005). A subset of radio interfaces on these nodes is used for providing network access to end-devices, whereas other radio interfaces are used to relay packets to the nearest Internet Gateway.

Experimental 802.11b/g mesh network developed at the MIT Computer Science and Artificial Intelligence Laboratory is described in (MIT Roofnet Project, 2009). Currently consisting of a network with 20 active nodes, Roofnet provides broadband internet access to users in Cambridge.

The MobiMESH architecture has been implemented in a real-life testbed in the Advanced Network Technologies Lab at the Politecnico di Milano as explained in (Capone, et al, 2006). The architecture is designed to seamlessly apply the 802.11 standard to its nodes. Seamless mobility is the primary issue, since wireless local area network (WLAN) clients roam within the coverage area of the mesh without losing connectivity.

A wireless mesh network developed at Carleton University is introduced in (Wireless mesh networking, 2009.) The wireless mesh network architecture consists of two parts: the mesh backbone and local footprints. All the mesh nodes are equipped with two wireless interfaces. One is an IEEE 802.11a/g compliant radio, which is the backbone traffic carrier. Another is an IEEE 802.11b radio, which provides access to wireless clients within the local footprint.

The wireless mesh network testbed, called MeshDVNet, which was developed in the LIP6 laboratory of the Université Pierre et Marie Curie, is presented in (Infradio project, 2009). This work is mainly concerned with the development of an efficient cross-layer routing protocol to increase the transport capacity of the mesh backbone as much as possible. The proposal also considers more efficiently managing user mobility. Both tasks have been integrated in MeshDV, a unique framework that is supported by a two-tier WMN architecture.

The feasibility of deploying a community mesh network to share broadband Internet access in a rural neighborhood with stationary nodes is described in (Wayne, et al. 2005). They examine the feasibility of constructing a community mesh network in a rural neighborhood at Dartmouth College using off-the-shelf hardware and software components without using an outdoor antenna. In addition, they identify several challenges related to the construction of such networks including network density, hardware limitations, and the US electrical code.

The testbeds evaluated have several drawbacks: the work reported in (Ramachandran, 2005) uses multi-radios network nodes, which significantly increases the cost and design complexity of the routing protocols. A negative aspect of the testbed presented in (MIT Roofnet Project, 2009) is that it considers a modified version of the dynamic source routing (DSR) Protocol, which increases header size and latency due to its routing mechanism. The work reported in (Capone, et al, 2006) utilizes a proactive routing protocol and requires two radio interfaces, which may not be suitable for highly dynamic wireless networks. The testbeds described in (Wireless mesh networking, 2009), (Infradio project, 2009), and (Wayne, et al, 2005) employ two wireless

interfaces. In short, all of the testbeds evaluated in this study use at least two wireless interfaces, one to connect to the backbone and the other to connect to the users.

The Pandora protocol is designed to make use of a single wireless interface (Aquino-Santos, et al, 2009). The performance results demonstrate that the use of a single interface does not affect the performance of a wireless mesh network.

SOCIAL ISSUES IN THE APPLICATION OF MOBILE AND LOCAL WIRELESS NETWORKS

Since the advent of electronic bulletin board systems (BBS) and the Internet, people have created and used a number of ways to communicate and socialize online. Today, people using traditional and wireless Internet connections demand increasingly greater bandwidth as they employ a greater variety of network technologies (Wi-Fi) and communicate through peer-to-peer connections, such as Bluetooth. Hotspots (sites that offer paid or free Internet access to their visitors over a wireless local area network) and other types of local area networks (LANs) are available in many public areas (e.g. cafes, malls, government offices, and hotels, among others) and in private sites (e.g. schools, houses, etc.). These hotspots use Wi-Fi technology, access points, routers and bridges connected to digital subscriber telephone connection lines (DSL) or cable modems, using fixed infrastructure connected to an Internet Service provider (ISP) (Rao and Parikh, 2003).

People increasingly use cellular phones, pocket computers, notebooks, laptops and other mobile electronic devices to connect to public and private wireless LANS, communicating though text messaging, voice over IP (VoIP), and recently over video conferences. One of these mobile devices is the so-called smart phone, which allows people to communicate across different network interfaces, including wireless networks with Internet connectivity, cellular phone connections, and peer-to-peer communications at short distances using Bluetooth, among others (Motani et al., 2005). People use mobile devices and wireless networks mainly to socialize, entertain, keep in touch with family and friends, study, and work, among other activities, communicating through online social networks.

An online social network can be defined as a group of individuals or organizations called nodes that use the Internet as a communication medium, forming a social structure with a series of particular social relations. Many people who participate in online social networks have used wireless networks for online access to the Internet, and rely heavily on mobile computing with access to various wireless networks, communicating and collaborating massively with the use of text, images, sound and video within a social network. The use of wireless social networks has allowed people to communicate almost anytime and anywhere (Smith, 2000).

There are emerging types of online social networks in the form of collaborative virtual worlds. A virtual world is an online and three-dimensional graphical space, where people communicate and collaborate together thorough graphical personifications called avatars.

In addition to text messages and VoIP, people use gestures to communicate in virtual worlds. However, virtual worlds generally require large, fast, and reliable network broadband connections. It is possible that virtual worlds can be used to support critical applications that require stable and efficient network access, for example, the analysis of information on a disaster area, to analyze the extent of the damage and to support decision making, among other applications. Therefore, a wireless mesh networks such as the Pandora architecture can be used to efficiently support wireless connections in virtual worlds and simulated environments.

Nevertheless, the increasing number of users of mobile devices and social networks has led to an ever increasing demand in both the number of connections, increased bandwidth, and improved quality of service (QoS), among other technical requirements (Rao and Parikh, 2003). In addition, people devise, implement, and use new and more complex online social networks such as virtual worlds, which require much improved wireless and wired network connections, and sometimes these types of requirements cannot always be available.

There are a number of users that need to keep communicated in special situations, such as people who work and live in rough and remote places. Improving communication among these isolated social groups that have been affected by armed conflict is of vital importance. In these cases, the distance and type of terrain separating user from the nearest Internet node does not allow efficient transmission of conventional networks, such as cellular phone signals and WiFi networks. In those conditions, such networks can be unstable, sometimes with poor QoS and limited bandwidth. This can severely limit communications with family, friends, co-workers, and the outside world, in general, causing delays and affecting collaborations with other remote social networks as well. In addition, there can be limited contact between common users and government agencies, humanitarian caregivers, education, and counseling providers, among other types of activities where social interaction is involved. It is possible to install and use some types of wireless connections such as radio frequency links, satellite connections, and WiMAX to access the Internet and wide area networks (WANs), but these solutions are expensive and are not always reliable, since some types of climates and terrains can affect their transmissions, and some of these solutions require a considerable amount of energy to function (Bertoni, 1999).

PANDORA PROTOCOL

Pandora is a routing protocol for wireless mesh networks. The backbone nodes employ a proactive routing strategy, which is based on an adaptation of the Dijkstra Algorithm, also known as Dijkstra's Shortest-path Algorithm. The Pandora routing protocol (PRP) includes an Internet Root (IROOT) node, which is the Pandora root node. The IROOT node is in charge of setting up the mesh configuration. As a result, the network topology cannot be established without the aid of this device.

The Pandora protocol has been designed for rural and emergency wireless networks where no physical infrastructure exists. It was developed in C language under the Ubuntu 2.6.15 Linux platform. Figure 1 shows the hierarchical network architecture employed by the Pandora protocol. Two different types of nodes are part of the Level 1: IROOT and Network Backbone (NBB). Level 2 is formed by Network Root (NROOT) nodes and Level 3 is formed by leaf nodes.

The IROOT node is equipped with two interfaces, one which has a link to the Internet and another that is connected to the NBB nodes that form the mesh backbone at the Level 1. NROOTs, in Level 2, are actually gateways between NBB nodes and leaf nodes. Level 3, the final level of the Pandora architecture, consists of leaf nodes that have limited energy, processing and transmission resources. Finally, there is another node called undecided, which is the initial state of all network nodes before they become NBB, NROOT or leaf nodes.

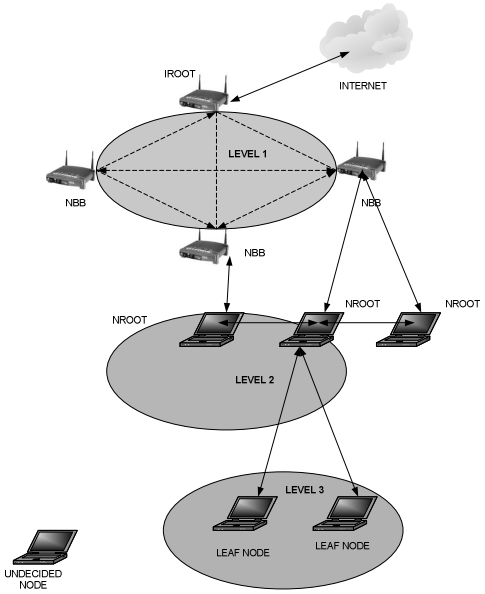


Figure 1: Hierarchical network architecture employed by the Pandora Protocol

Routing protocol

The Pandora routing protocol aims to achieve a main goal: it tries to make optimal use of high capacity mesh routers in a hybrid WMN by routing packets along paths consisting of mesh routers whenever possible. This not only increases the overall throughput and reduces latency; it also helps to conserve battery power of client devices. It employs several metrics at two levels: bandwidth utilization, residual battery energy monitoring, geographic location, and the number of users.

Group formation at level 1 (NBB node)

1. The IROOT node executes a script to obtain its Internet protocol (IP) address and configuration parameters for its wireless interface, including the medium access control (MAC) address, geographical location, and a time stamp, as well as information about the residual battery energy and bandwidth utilization.
2. Then, the IROOT node changes its flag status to B, indicating that this is the root node with access to the Internet.

3. Next, the IROOT node clears the neighbor table and starts the routing function.
4. The undecided node then sends Hello packets asking other nodes to join the IROOT.
5. After this, the undecided node joins the IROOT and changes its state to a NBB node.
6. The NBB node then collects information from neighbor nodes and sends it to the IROOT, which adds the information to the main table.
7. Finally, the IROOT node forwards the main table to its neighboring NBB nodes. With this information, each NBB node obtains a complete view of the network.

Routing at level 1

NBB nodes broadcast small packets every 5 seconds to indicate they are "alive." If a NBB node (source node) needs to inform its NBB neighbor nodes of network changes, including nodes entering and exiting the network, it will send a larger packet containing the identifications (IDs) of all new neighbor nodes. The large packet will include the geographical position of all new neighbor nodes, the residual battery energy, and the bandwidth utilization, which will be retransmitted to all NBB neighbor nodes until the packet reaches the IROOT node (destination node).

Group formation at level 2 (NROOT node)

Several conditions need to be met to convert an Undecided node to an NROOT node.
A NBB node verifies that its maximum number of NROOT nodes has not been reached.
The Undecided node executes three steps:

1. First, is sends a Hello packet every second.
2. If the Hello packet is reached by one NBB node, the NBB node replies to the Undecided node.
3. Finally, the Undecided node asks to be member of the NBB node. If the Undecided node receives a positive reply from the NBB node, the Undecided node becomes an NROOT node.

Routing at level 2 within the same group

The NROOT node has the information of all its Leaf nodes. Furthermore, each Leaf node also has the information of each neighbor Leaf node and its NROOT node. Thus, when a Leaf node source sends information to another Leaf node destination in the same group, the Leaf node sends the packet directly to the destination Leaf node.

Routing at level 2, neighbor group

This is the case when one Leaf node wants to communicate with another Leaf node, but they belong to different NROOT nodes. The procedure is as follows: the Leaf node source searches in its routing tables. If the source Leaf node has the Leaf node destination in its routing table, the source Leaf node sends the packet directly to the destination Leaf node. Otherwise, the source Leaf node sends the packet to its NBB root node through its NROOT node. The NBB node asks its NBB neighbor nodes if they have registered the destination Leaf node. After this, if a NBB node finds the destination Leaf node in its routing table, it replies to the originating NBB node. Then the originating NBB node sends to its Leaf node the address of the destination Leaf node. Finally, the source Leaf node starts the communication process with the destination Leaf node.

Group formation at level 3 (leaf node)

Several conditions need to be met to convert an Undecided node to a Leaf node.
A NROOT node verifies that its maximum number of Leaf nodes has not been reached.
The Undecided node then executes two steps:

1. First, the Undecided node sends a Hello packet every second.
2. If the Hello packet is reached by one NROOT node, the NROOT node replies to the Undecided node. Then, the Undecided node asks to become a member of the NROOT node. If the NROOT node replies to the Undecided node with a positive acknowledgement, the Undecided node changes its status to a Leaf node.

More detailed information concerning the Pandora protocol can be found in (Cosio-León, et al, 2008).

TESTING THE PANDORA PROTOCOL

Pandora was developed and tested on a Linux system using Ubuntu with 2.6.15 and 2.6.17 kernels, both with and without QoS.
In this work, we present the results of bandwidth and jitter with several types of traffic and two packet sizes. The available network bandwidth is employed to determine network capacity. The Pandora evaluation considers different types data traffic which have different constrains in terms of bandwidth and jitter. The traffic sources include: only data (TCP), data + voice, data + voice + video and UDP without Marks.

Queuing disciplines used in the Pandora protocol

The PRIO, HTB, and DSMARK queuing disciplines are used to evaluate if bandwidth and jitter are improved. The PRIO qdisc is a classful queuing discipline that contains an arbitrary number of classes with different priorities. When a packet is enqueued, a sub-qdisc is chosen based on a filter command that is given in tcng (Traffic Control Next Generation, 2009). HTB is a more understandable, intuitive and faster replacement for the class-based queuing (CBQ) qdisc in Linux. Both CBQ and HTB help control outbound bandwidth on a given link. Both use one physical link to simulate several slower links and to send different kinds of traffic to different simulated links. DSMARK is a queuing discipline that offers the capabilities needed in differentiated services (also called DiffServ, or simply, DS). DiffServ, along with integrated services, is one of two actual QoS architectures that are based on a value carried by packets in the DS field of the IP header.

Tools employed in the evaluation of the Pandora protocol

Two different tools were used to evaluate the Pandora protocol: IPERF (IPERF, 2009) and echoping (Echoping, 2009). IPERF is a traffic injector that reports bandwidth, jitter, and traffic behavior for TCP and UDP. Echoping permits one to measure network traffic delays.

Testbeds utilized for evaluating QoS in Pandora protocol

Figure 2 shows the two scenarios employed in the evaluation of the Pandora protocol. In Scenario 1, three laptops were used, with one of them configured as the IROOT node and the other two as NBB nodes. Scenario 2 used for evaluating the Pandora protocol considered three levels with four laptops, one of which functioned as an IROOT node, another as a NBB node, another as a

NROOT and the final laptop functioning as a leaf node. Packet sizes of 1024 and 2024 were employed to evaluate the performance of the Pandora protocol.

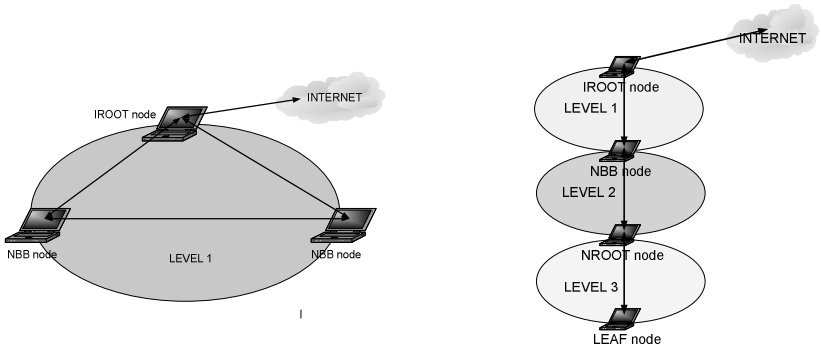


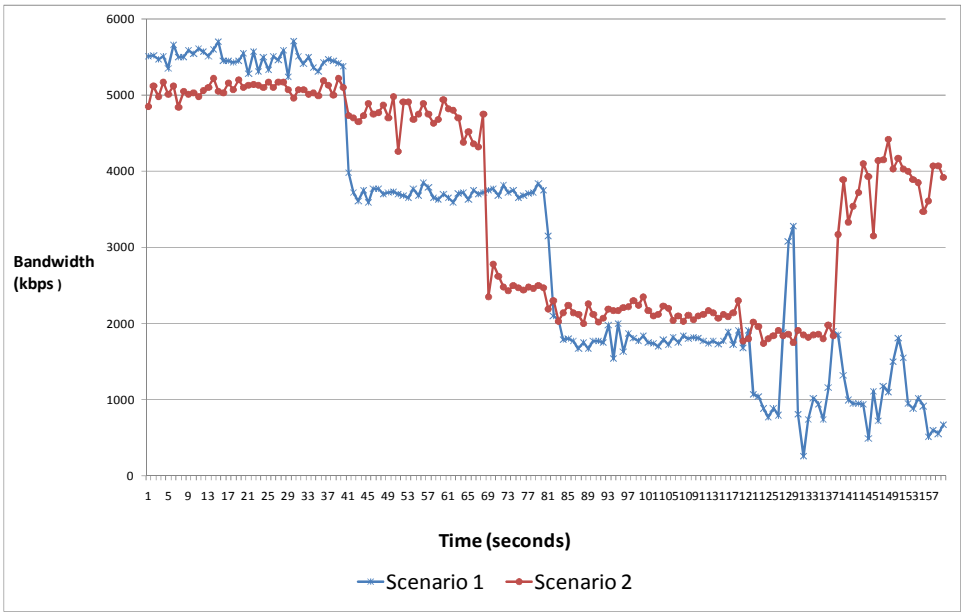
Figure 2: Scenarios 1 and 2, used to evaluate the Pandora protocol.

Analysis of results of the Pandora protocol

Figure 3 shows the bandwidth utilized by different traffic flows injected into both scenarios with IPERF. Traffic is injected into the network without any queuing discipline. The TCP traffic flow starts at second 0, audio transmission initiates at 40 seconds and video streaming begins at 80, with UDP traffic flow commencing at 120 seconds.

At the beginning, when only data are being transmitted, 1024-byte packets affect bandwidth only slightly more than in Scenario 1. However, when data + audio are being transmitted, Scenario 1 is affected less. When data + audio + video are being transmitted, including UDP traffic, Scenario 1 performs better in terms of bandwidth.

On the other hand, when packet sizes of 2024 bytes are being transmitted, Scenario 1 is affected a slightly more. The hierarchical organization of Pandora performs better in terms of network bandwidth when larger packet sizes are being transmitted.



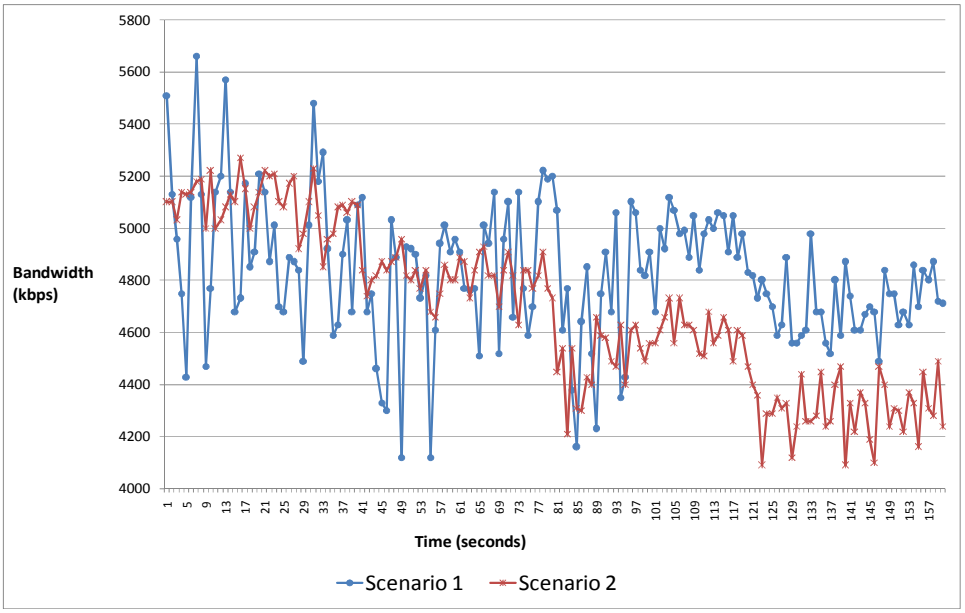
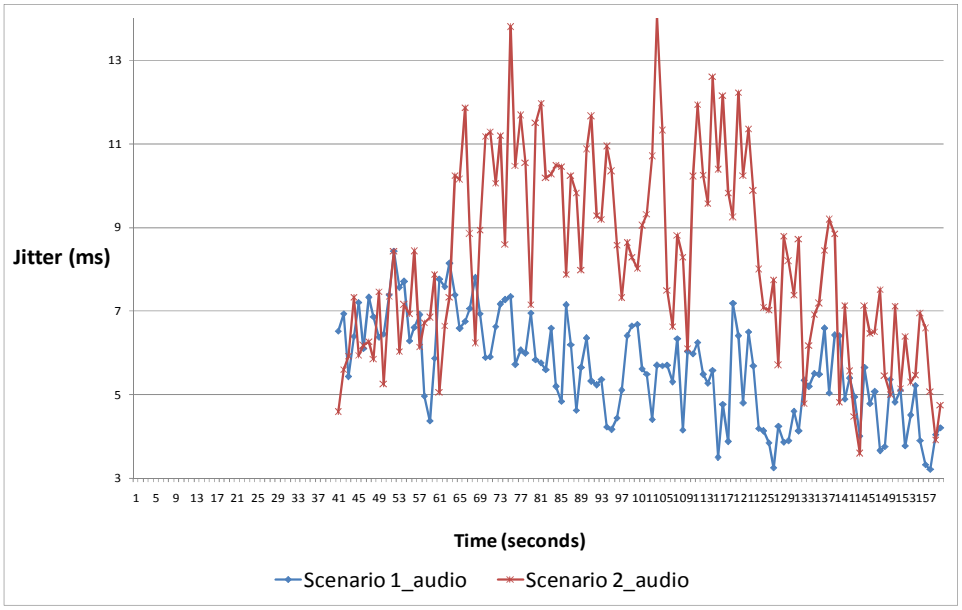


Figure 3: Bandwidth used by different traffic flows without applying any queuing discipline, employing 1024 and 2024-byte packet sizes.

Figure 4 shows the Jitter for the traffic flow injected into both scenarios. Traffic flows are injected into the network without applying a queuing discipline. The jitter is under the minimum recommended margin of 100 ms. for quality of service (QoS) applications in all packet sizes. However, packet sizes of 1024-bytes perform better for Scenario 1 without applying any queuing discipline. For packet sizes of 2024, both scenarios perform similarly.



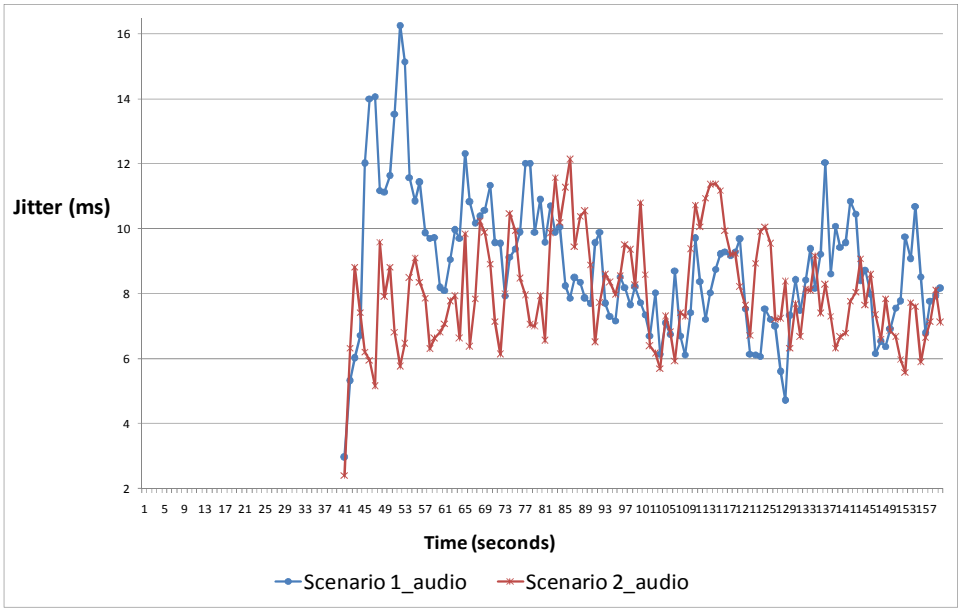
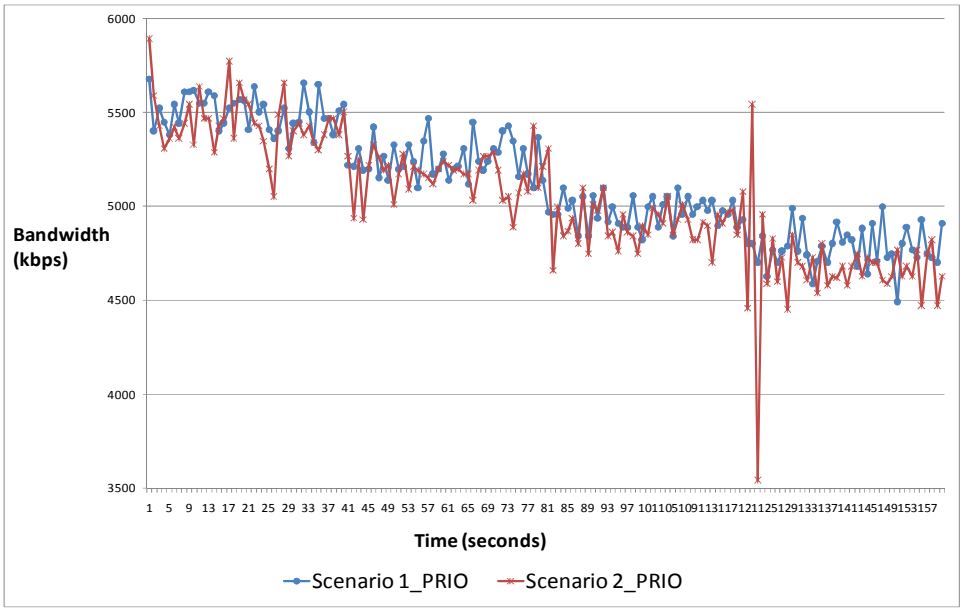


Figure 4: Jitter for different traffic flows without applying any queuing discipline, employing 1024 and 2024-byte packet sizes.

Figure 5 shows the bandwidth utilized for the different traffic flows injected into both scenarios, utilizing a PRIO qdisc. Network performance is very similar for scenarios with1024 and 2024-byte packet sizes, meaning that PRIO qdisc efficiently manages network bandwidth for both scenarios.



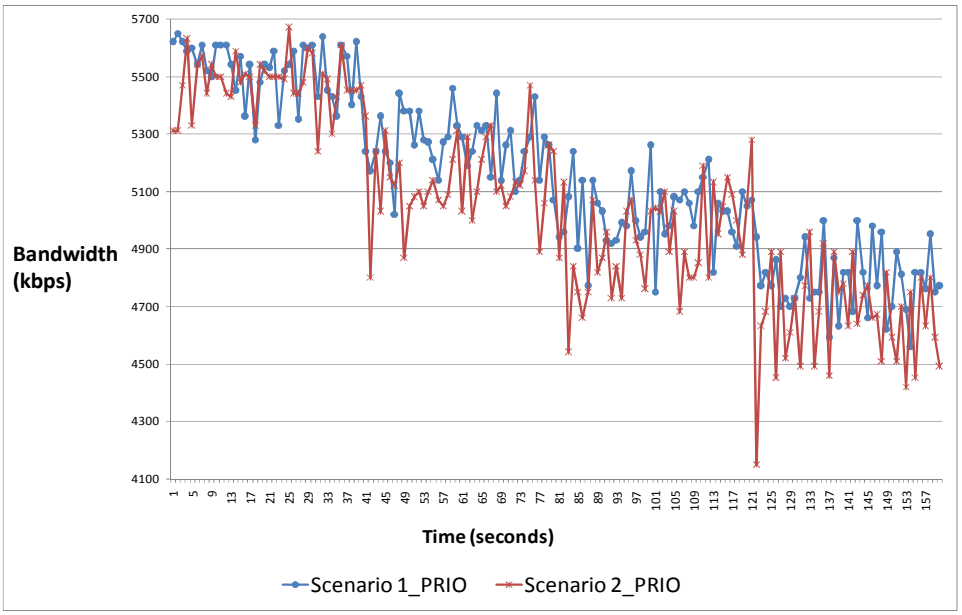
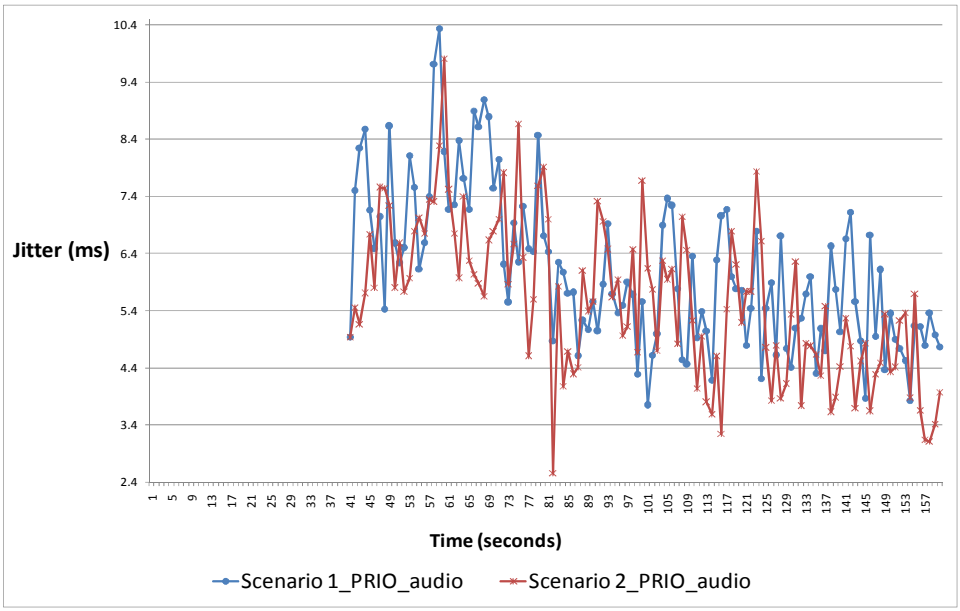


Figure 5: Bandwidth used by different traffic flows with PRIO qdisc, employing 1024 and 2024-byte packet sizes.

Figure 6 shows the Jitter for the traffic flow injected into both scenarios. The jitter is under the minimum recommended margin of 100 ms. for QoS applications in all packet sizes.



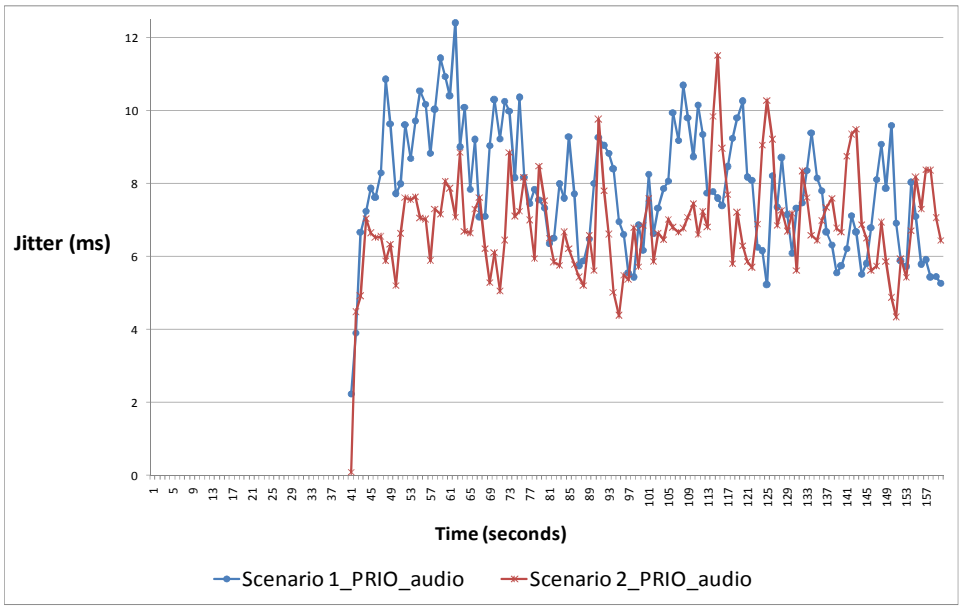
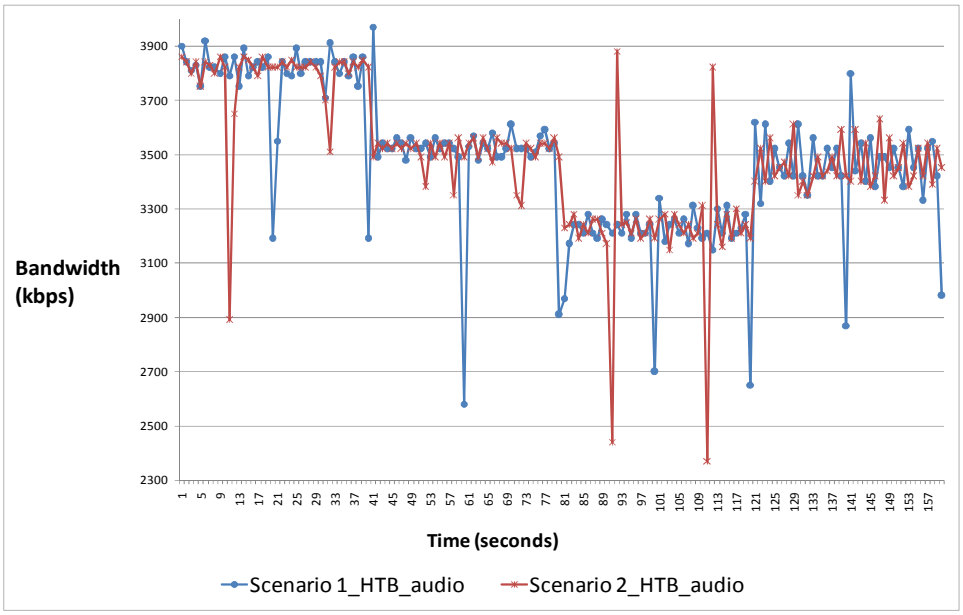


Figure 6: Jitter for different traffic flows utilizing PRIO qdisc, employing 1024 and 2024-byte packet sizes.

Figure 7 shows the bandwidth utilized for the different traffic flows injected into both scenarios utilizing a HTB qdisc and prioritizing audio flow. For packet sizes of 1024 and 2024, the network bandwidth is handled efficiently by HTB qdisc.



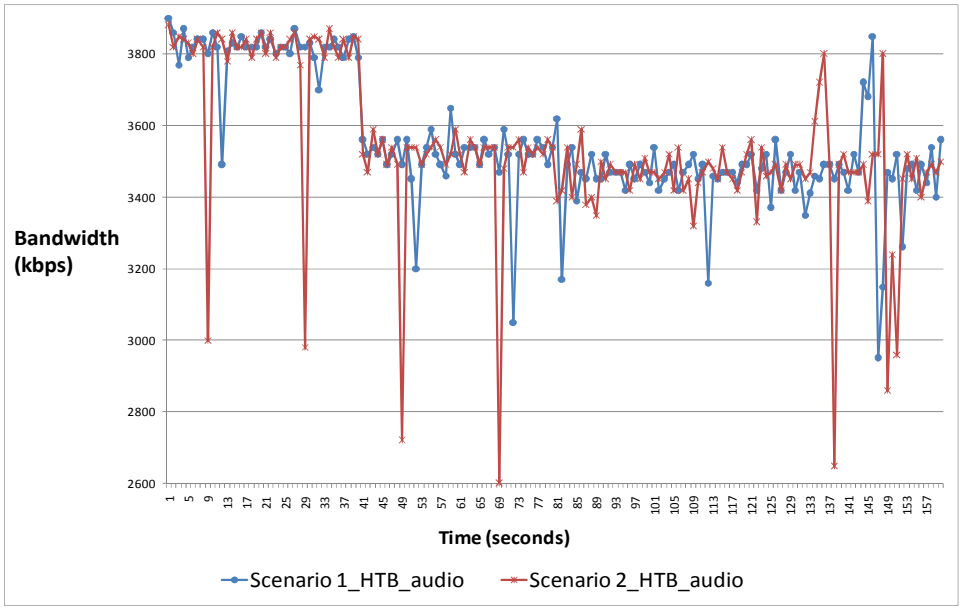
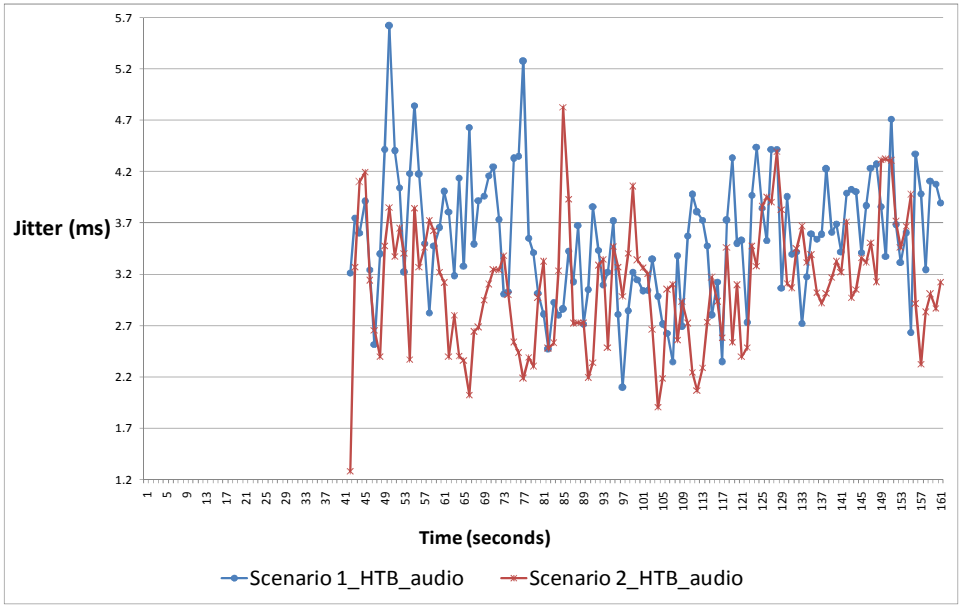


Figure 7: Bandwidth used for different traffic flows with HTB qdisc prioritizing audio flow, employing 1024 and 2024-byte packet sizes.

Figure 8 shows the Jitter for different traffic flows injected into both scenarios with HTB qdisc prioritizing audio. With 1024 and 2024-byte packet sizes, the jitter is lightly affected in the both scenarios.



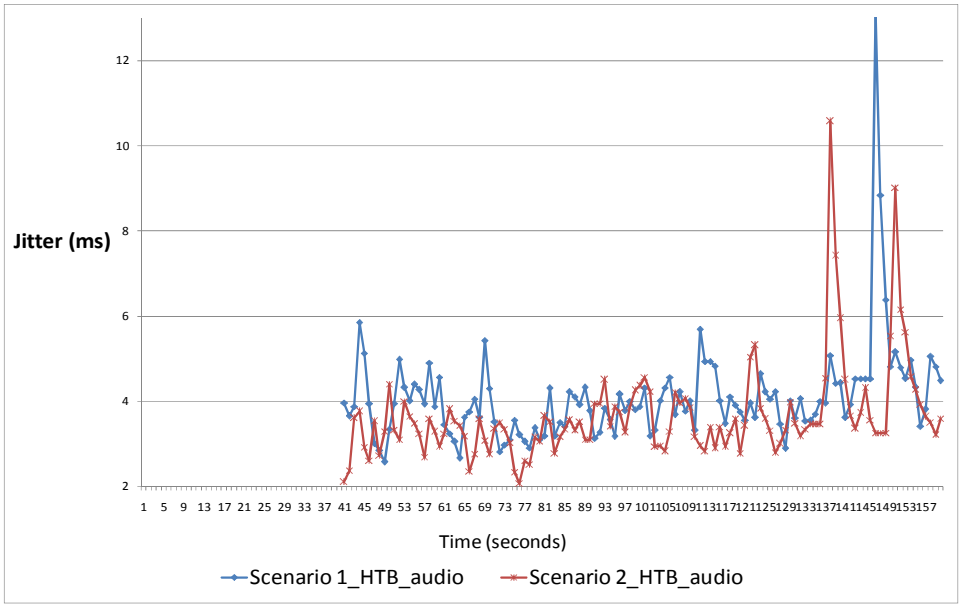
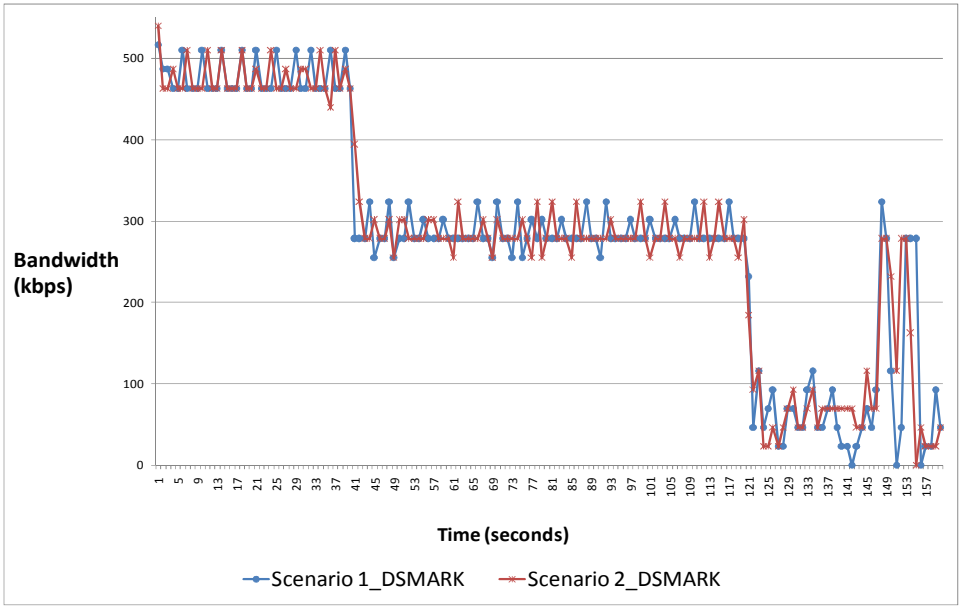


Figure 8: Jitter used for different traffic flows with HTB qdisc prioritizing audio flow, employing 1024 and 2024-byte packets.

Figure 9 shows the bandwidth utilized for the different traffic flows injected into both scenarios utilizing a DSMARK qdisc. DSMARK qdisc allows both packet sizes to share the network bandwidth similarly.



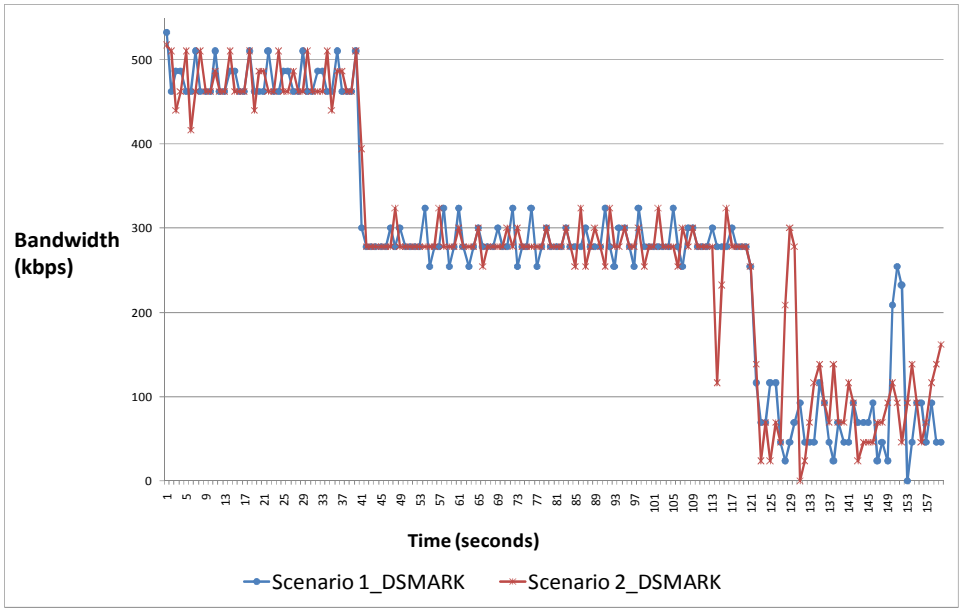
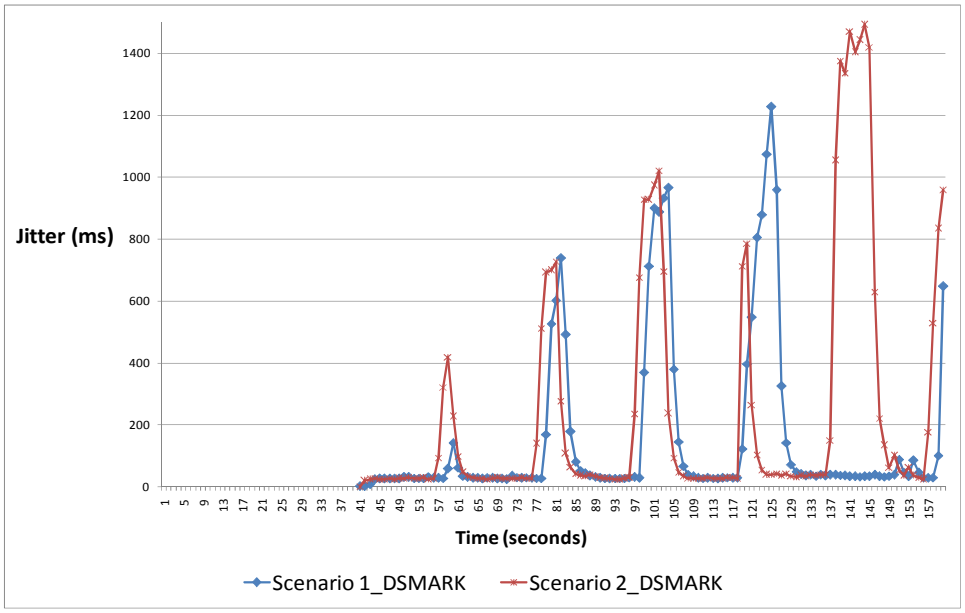


Figure 9: Bandwidth used for the different traffic flows with DSMARK qdisc, 1024, 2024-byte packet sizes.

Figure 10 shows the Jitter for different traffic flows injected into both scenarios with DSMARK. The performance of the network is considerably affected with both packet sizes in both scenarios.



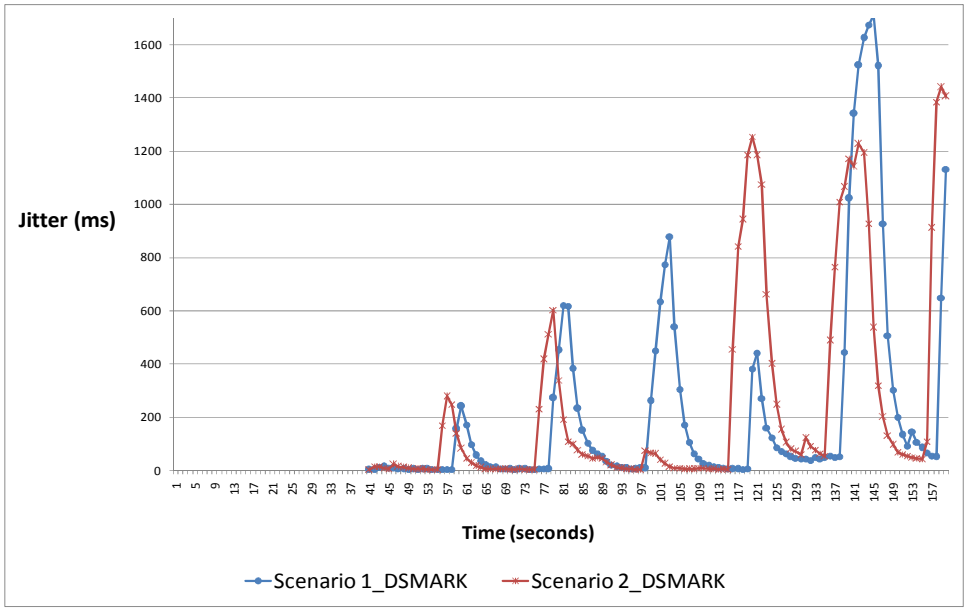


Figure 10: Jitter for different traffic flows with DSMARK qdisc, employing 1024, and 2024-byte packet sizes.

TESTBEDS UTILIZED FOR EVALUATING THROUGHPUT AND END-TO-END DELAY IN THE PANDORA PROTOCOL

The tests were carried out in two stages. The first stage considered the installation of the Pandora protocol in Laptops with the objective of evaluating the end-to-end delay (EED) and the throughput metrics (Ramachandran, et al, 2005). In the second stage, Pandora was installed on a wireless router (ASUS WL-500gPremium) and the metrics measured were route regeneration time and the time required for nodes to enter and exit the backbone.

Laptops scenarios

In order to measure the end-to-end delay (EED) and throughput, during the first stage of testing, different configurations with laptops at 1, 2 and 3 hops were evaluated. First, the routes were configured manually and the two tests consisted of sending 100 pings to a node at 1, 2 or 3 hops with 84 byte and 1000 byte packets, respectively. The distance between laptops 1 and 2 was 25 meters. The distance between laptops 2 and 3 was 50 meters and, finally, the distance between laptops 3 and 4 was again 25 meters. Laptops 1, 2 and 3 were located without line of sight and laptops 3 and 4 were placed with line of sight. The purpose of locating laptops 1, 2, and 3 without line of sight was to increase the distance between them.

The second test stage followed the same procedure as the first. However, Pandora's route selection protocol was employed to establish communication between the laptops. The separation and location of the laptops was identical to the abovementioned first test stage. The specific deployment is shown below in Figure 11.

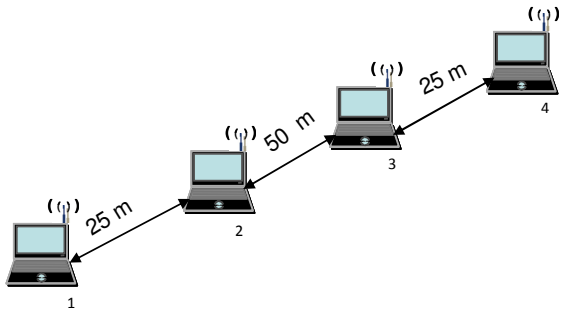


Figure 11: Localization of laptops for the first stage.

To determine throughput, a 3489 Kbyte file was sent via "sftp" and the reception time was registered. This throughput experiment was realized for 1, 2 and 3 hops, both manually and with the Pandora algorithm.

Wireless routers

The router tests were carried out indoors with the laptops within line of sight as shown in Figure 12.

The first node added as a precursor to the backbone was the "IROOT." After that, the NBB nodes were added one by one to give the actual structure shown in Figure 12. After forming the backbone, the nodes were alternatively enabled and disabled in a programmed sequence in order to insure that route regeneration did not add significant end-to-end delay between the laptop (node) and the nBB.1.

We used the Mexican National Autonomous University's (UNAM, in Spanish) online radio station to maintain a constant audio and video transmission stream to monitor the behavior of the Pandora algorithm.

Each ASUS WL-500gPremium routers were preconfigured according to the settings detailed below:

	IROOT.4	NBB.1	NBB.2	NBB.3
IP	192.168.4.4	192.168.4.1	192.168.4.2	192.168.4.3
BSSID	Pencil	Pencil	Pencil	Pencil
Mode	Ad-hoc	Ad-hoc	Ad-hoc	Ad-hoc

Table 1: Basic configuration for the wireless routers used in the testbed.

Backbone formation

Nodes were added one by one with the Iroot.4 running to form the structure detailed in Figure 12.

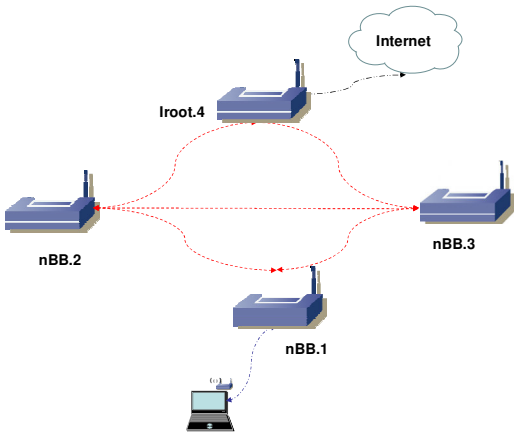


Figure 12: Testbed with line of sight between routers.

Route regeneration

The first test to determine route regeneration was to turn off the nBB.2 once the structure was formed because turning off the nBB.2 forces all the others nodes to reroute their paths between Iroot.4 and nBB.1.

The following step was to turn off nBB.3 to obtain the reset time for nBB.1. Once nBB.1 was assigned undecided status, nBB.2 was once again turned on to obtain the time of convergence.

1. ANALYSIS OF RESULTS OF THE PANDORA PROTOCOL

Laptops

Results in Figure 13 show that there was no significant difference with regards to end-to-end delay with a packet size of 84 bytes. The results for 1028-byte packets were very similar. Figure 14 illustrates the differences for 1, 2 and 3 hops.

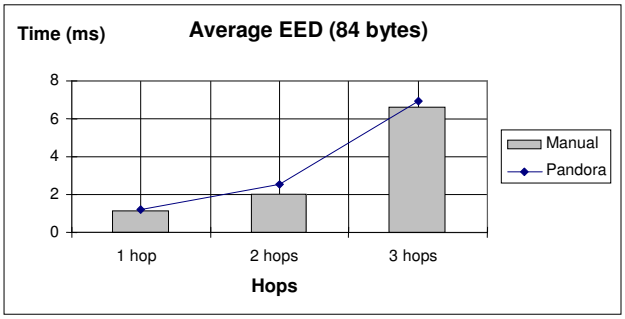


Figure 13: Comparative EED results in 84-byte packets.

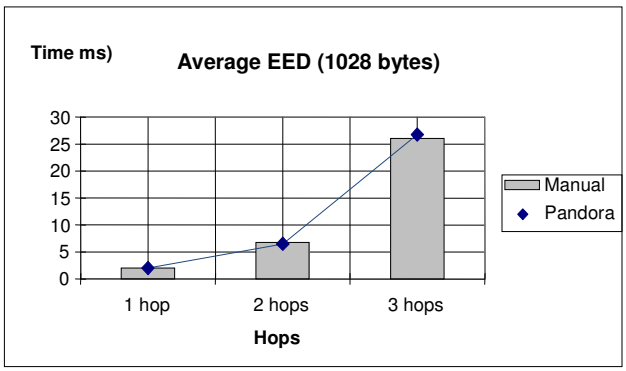


Figure 14: Average EED for 1028-byte packets.

Figures 15 and 16 show the maximum EED and the average EED for 84- and 1028-byte packets.

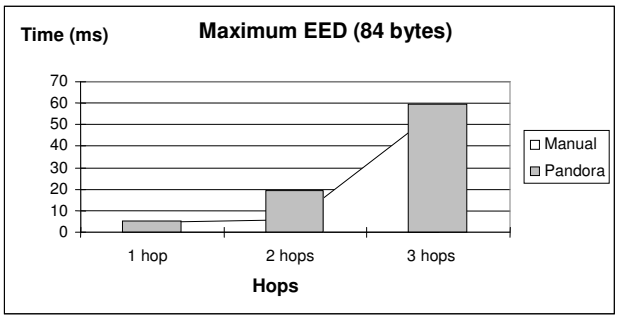


Figure 15: Maximum EED for 84-byte packet.

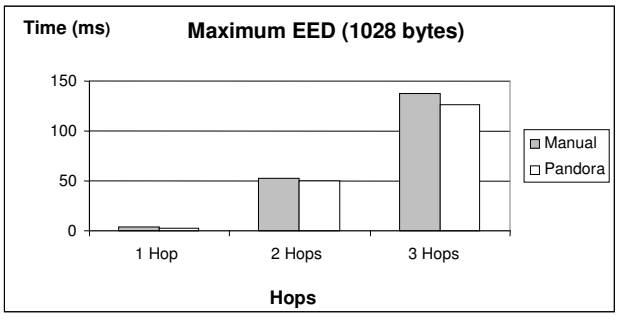


Figure 16: Maximum EED with 1028-byte packet.

Figure 17 shows that Pandora does not introduce any significant delay in terms of throughput.

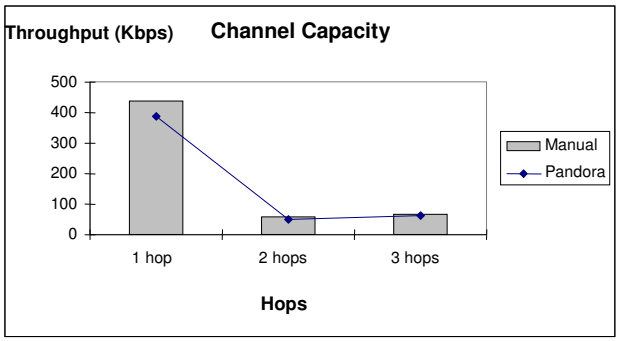


Figure 17: Throughput in the Pandora protocol.

Wireless routers

The time required to delete a specific node from the neighbor tables is called the table update time and the measure for this parameter was 7 seconds.

The time a node needs to register a new neighbor is called the register time. For Pandora, this time varied between 3 and 6 seconds, and depended on whether the backbone node received the Hello packet as soon as the Undecided node turned on, or if it was received one second later.

The one-hop regeneration time was less than 8 seconds and the two-hop regeneration time was 13 seconds.

The time required for regeneration is directly proportional to the time required for the Hello packet to be transmitted. If the processing time for Hello packets is reduced, more Hello packets can be sent in the same amount of time. However, because the backbone has such low mobility, increasing the number of Hello packets could result in traffic overload and reduced network performance.

Using Pandora, the UNAM radio transmission was not interrupted to the laptop attached to nbb.1. Furthermore, throughput tests show no breaks in communication.

2. CONCLUSIONS

This chapter described the Pandora routing protocol, which is appropriate for hybrid wireless mesh networks (HWMN). The routing heuristic employed by the Pandora protocol takes into consideration some of the most important parameters required for a wireless network, which include: geographical localization, residual battery energy, bandwidth utilization and the number of users. The Dijkstra algorithm allows Pandora to create excellent and stable paths that insure a uniform use of network resources.

The performance evaluation of the Pandora protocol included the implementation of different queuing disciplines, including: PRIO, HTB and DSMARK. The PRIO, HTB, and DSMARK queuing disciplines were tested for TCP, voice, video, and UDP traffic in two different scenarios, and the three queuing disciplines were tested using 64, 1024, and 2024-byte packet sizes. Results show that traffic flow was not significantly affected when QoS was not taken into account

because Pandora considers bandwidth utilization as part of its routing strategy. When employing the different queuing disciplines, it was observed that PRIO and HTB prioritizing UDP performed the best.

Some additional testbed scenarios were setup to test the performance of Pandora, one with laptops and the other with commercial wireless routers (ASUS WL-500g Premium). Results show that Pandora does not add a significant load to the network traffic and, therefore, does not increase end-to-end delay. Furthermore, its self-constructing and self-healing capacity does not significantly impact network performance, which is a very important virtue in emergency situations where network autonomy is crucial.

Performance results also demonstrate that network performance is not affected when the network devices are equipped with a single wireless interface when employing the Pandora protocol.

In summary, an important characteristic of Pandora is that it performs well in laptops and embedded systems. Future research will include how to incorporate Pandora in wireless mesh sensor networks.

References

Aquino-Santos, R., González-Potes, A., García-Ruiz, M. A., Rangel-Licea, V., Villaseñor-González L. A., Edwards-Block, (2009). A. Hybrid Routing Algorithm for Emergency and Rural Wireless Networks. Electronics and Electrical Engineering Journal, vol. 89, num. 1, pp. 3-8.

Bertoni, H.L. (1999). Radio Propagation for Modern Wireless Systems. Prentice Hall Professional Technical Reference, New York.

Braunstein, B., Trimble, T., Mishra, R., Manoj, B. S., and Rao, R. (2006). On the Traffic Behavior of Distributed Wireless Mesh Networks. Proceedings of the International Symposium on a Worl of Wireless, Mobile and Multimedia Networks, (WoWMoM), pp. 1-6.

Capone, A., Napoli, S., and Pollastro, A. (2006). MobiMESH: An Experimental Platform for Wireless MESH Networks with Mobility Support. Proceedings of ACM QShine, pp. 1-6.

Cosio-León, M., Galaviz-Mosqueda, G., Aquino-Santos, R., Villaseñor-González, L., Sánchez-García, J., Gallardo-López, J. (2008). Protocolo PANDORA: Implementación y pruebas en computadoras portátiles y sistemas embebidos ASUS WL-500gP. Centro de Investigación Científica y de Educación Superior de Ensenada, CICESE, pp. 1-43.

Echoping. (2009). http://echoping.sourceforge.net/. Last access on September, 15, 2009.

Grace, K. (2000). Mobile Mesh Border Discovery Protocol. Work in Progress. (Internet Draft) http://www.mitre.org/work/tech_transfer/mobilemesh/draft-grace-manet-mmrp-00.txt

IPERF. (2009). http://iperf.sourceforge.net/. Last access on September, 15, 2009.

LIP6-UPMC RNRT Infradio Project. [online]. Available:
http://rnrt-infradio.lip6.fr/indexEnglish.html

"MIT Roofnet Project", [online]. Available:
http://pdos.csail.mit.edu/roofnet/doku.php

Motani, M., Srinivasan, V., and Nuggehalli, P.S. (2005) .Peoplenet: Engineering a Wireless Virtual Social Network. Proceedings of the 11th annual international conference on Mobile computing and networking, pp. 243-257.

Ogier, R., Templin, F., Lewis, M. (2004). Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). Work in Progress.
http://www.faqs.org/rfcs/rfc3684.html

Pirzada, A. A; Portmann, M; Indulska, J. (2006). Performance Comparison of Multi-Path AODV and DSR Protocols in Hybrid Mesh Networks. 14th IEEE International Conference on Networks, pp. 1-6.

Pirzada, A. A; Portmann, M; Indulska, J. Hybrid Mesh Ad-hoc On-demand Distance Vector. Proceeding of the Thirtieth Australasian Conference on Computer Science, pp. 49-58, 2007.

Portmann, M., and Pirzada, A. (2008). Wireless Mesh Networks for Public Safety and Crisis Management Applications. IEEE Internet Computing, vol, 12, pp. 18-25.

Ramachandran, K., Buddhikot, M., Chandranmenon, G., Miller, S., Belding-Royer, E., and Almeroth, K. (2005). On the Design and Implementation of Infrastructure Mesh Networks, IEEE Workshop on Wireless Mesh Networks (WiMesh), pp. 1 -12.

Rao, B., and Parikh, M.A. (2003). Wireless Broadband Drivers and their Social Implications. Technology in Society, 25, pp. 477-489.

Smith, M. (2000). Some Social Implications of Ubiquitous Wireless Networks. ACM SIGMOBILE Mobile Computing and Communications Review, 4(2), pp 25-36.

Traffic Control Next Generation. (2009). http://tcng.sourceforge.net/index.html
Last access on September, 15, 2009.

Wayne, A., Art, M., and Anand, R. Designing and Deploying a Rural Ad-Hoc Community Mesh Network Testbed. Proceedings of the IEEE Conference on Local Computer Networks, pp. 1-4, 2005.

Wireless mesh networking at Carleton University. [online]. Available:
http://kunz-pc.sce.carleton.ca/MESH/index.htm

Acronyms

AODV	Ad hoc On-demand Distance Vector
AODV-HM	An-hoc On-demand Distance Vector Hybrid Mesh
AOMDV	Ad hoc On-demand Multi-path Distance Vector
CBQ	Class-Based Queuing
DS	Differentiated Services
DSR-MP	Dynamic Source Routing Multi-Path
EED	End-to-End Delay
HTB	Hierarchical Token Bucket
ID	Identification
IP	Internet Protocol
IROOT	Internet Root
LSP	Link State Packet
MAC	Medium Access Control
MMBDP	Mobile Mesh Border Discovery Protocol
NBB	Network Backbone
NROOTs	Network Roots
PRP	Pandora Routing Protocol
PRIO	Priority Queuing Discipline
QoS	Quality of Service
TBRPF	Topology Dissemination Based on Reverse-Path Forwarding
TCP	Transport Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network