Providing Reliability and QoS in Multi-Hop Wireless Networks: The ADHOCSYS Approach

Paolo Bucciol, Luca Leschiutta
Dipartimento di Automatica e Informatica
Politecnico di Torino, Corso Duca degli Abruzzi, 24
10129, Torino, Italy
Phone: +39-011-090-7036, fax: +39-011-090-7198
E-mail: [paolo.bucciol,luca.leschiutta]@polito.it

Nikos Fragoulis
Electronics Laboratory – Dept. of Physics
University of Patras, Greece
Phone: +30-610997445
E-mail: nfrag@upatras.gr

Frank Y. Li
UniK – University Graduate Center
Instituttveien 25, Pb. 70, N-2027 Kjeller, Norway
Phone: +47-6484-4700
E-mail: frank.li@unik.no

Giampietro Zicca, Lorenzo Vandoni
Emisfera Società Cooperativa
Via dell'Industria, 25 - Fraz. Fondotoce, 28900 VB, Italy
Phone: +39+0323+586730
E-mail:[giampietrozicca,lorenzovandoni]@emisfera.it

ABSTRACT
Multi-hop wireless networks appear as a promising means for providing broadband Internet access in rural and mountain regions. Reliability and QoS are among others two important aspects in such context. This paper presents a pragmatic approach proposed by the IST FP6 ADHOCSYS project, which is supported by the European Commission under the IST strategic objective "Broadband for All". Starting from a general description of ADHOCSYS networks and application scenarios, the paper presents the methodologies adopted for providing reliability and Quality of Service (QoS) in such networks.

Categories and Subject Descriptors
C.2.1 [**Network Architecture and Design**]: Network Communications, Wireless communications

General Terms
[Algorithms, Design, Reliability, Experiment]

Keywords
Wireless networks, Internet access, network redundancy, reliability and availability, QoS, multi-homing.

1. INTRODUCTION
The main objective of the ADHOCSYS project is to provide a reliable broadband Internet access solution to people who live in rural and mountain regions where Digital Subscriber Line (DSL) is not available or non-profitable [2][5]. In towns or villages where Internet gateways are available, the ADHOCSYS networks will be used to provide broadband services to persons living outside these towns and villages. This objective is achieved by means of creating a reliable multi-hop wireless broadband network.

In the physical environment where the network will be deployed (for example in Italian mountain regions), inhabitants are typically aggregated in few dozens of small towns, villages and farms, which are several kilometers apart one from the other. This project considers situations where these home users are not reachable by DSL connections in the near future and other cases where people dwellings are spread apart in areas such that cable laying becomes impracticable or non-profitable for operators.

The network will provide end-users with access to a minimum set of services, for example e-mail and web browsing services in all circumstances, and allow higher level services, including broadband Internet access, IP Telephony etc under specific conditions. The main potential impact of the project is the fact that it provides a paradigm for providing broadband Internet services in rural and mountain regions, at an affordable price. The project contributes besides to a general enhancement of the state-of-the-art technologies about multi-hop wireless networks and lets the implementation of research results publicly available through an open source license available at [7].

The ADHOCSYS networks are organized in an ad hoc fashion through multi-hop wireless networks. Therefore, how to provide reliable services in such a network appears of utmost importance and a challenging task for the project. Although reliability in wired networks has been studied for many years [3], very little work can be found in the literature regarding reliability studies in wireless networks, especially for multi-hop wireless networks. On the other hand, QoS is always desirable when providing services to end-users, so special attention must be paid in any case in order to accommodate efficient QoS mechanisms.

MOBIMEDIA 2007, August 27-29, Nafpaktos, Greece

DOI 10.4108/ICST.MOBIMEDIA2007.1940

The idea behind providing reliability in ADHOCSYS networks is to introduce redundancies with the help of multiple gateways, redundant nodes and multiple channels. A smart routing algorithm has been used to exploit redundancy, and to allow for the network to continue working properly in case of failure of one or several nodes or links.

QoS mechanisms, on the other hand, allow the allocation and optimization of the different service strategies for various traffic flows, depending on the specific application class and requirements. The main goal of QoS provisioning in ADHOCSYS networks is to provide end-users with a network in which they can access an essential set of Internet services with satisfied expectations, and at the time, maximizing network utilization for other types of services.

The rest of this paper is organized as follows. Section 2 gives a description of ADHOCSYS network architecture and typical scenarios. Section 3 introduces our approaches to reliability prediction and QoS mechanisms. Section 4 presents the ADHOCSYS reliability prediction model, and then this reliability analysis and availability prediction model is applied to a few case studies with numerical results in Section 5. Finally, the concluding remarks are given in Section 6.

2. NETWORK ARCHITECTURE AND APPLICATION SCENARIOS

In the following, we describe briefly the network architecture, typical application scenarios in ADHOCSYS networks, before reliability and QoS considerations are presented in the next section. Other aspects of the project, such as routing, power supply, security and authentication, are not addressed in this paper. More detailed information on those topics can be found in [2] [3].

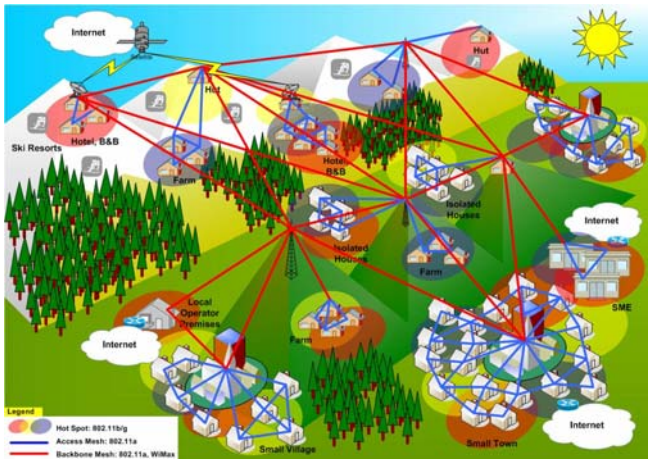

Figure 1. Typical ADHOCSYS network scenario.

2.1 Network architecture

An ADHOCSYS network might be large in terms of both geographic expansion and the number of nodes. Therefore a hierarchical architecture is needed to allow ADHOCSYS scaling from few dozens nodes to several hundreds, or even more, nodes. A 2-tier hierarchy is a good trade-off between network complexity and scalability.

Figure 1 illustrates the ADHOCSYS architecture and a typical application scenario. The first tier backbone network is represented in red, while the second tier mesh networks are represented in blue. The second tier nodes act also as APs for the end-users.

The first tier backbone network is a standard multi-hop wireless network consisting of several long wireless links. Long distances and short delays between transmitters and receivers will be achieved via IEEE 802.11 protocols directional antennas and fine tuning. The second tier network is a mesh access network which takes care of the physical (PHY) and Medium Access Control (MAC) layer issues in 802.11 wireless networks. The OLSR (Optimized Link State Routing) protocol is adopted in our networks with several enhancements implemented by the ADHOCSYS project. More detailed information regarding our OLSR enhancements can be found in [3].

It is worth mentioning that typical ADHOCSYS scenarios are based on static network topology, which is similar to mesh networking architecture. Mobile nodes are allowed as end-users, but they do not participate in routing.

2.2 Application scenarios

Various application scenarios have been envisaged for ADHOCSYS networks, as discussed in [1] [2]. However, only the primary application scenario defined in ADHOCSYS, which is targeted at providing broadband Internet access to rural and mountain areas through available gateway(s) at the edge(s) of towns and villages, is presented here.

The network is composed of several access networks interconnected by the backbone network.

Both the backbone and the access networks consist of a set of fixed access points organized in an ad hoc fashion, with redundant links. For both the backbone and the access networks, the adoption of standard 802.11a/b/g devices is envisaged. The backbone layer consists of long high-capacity wireless links connecting towns, villages, farms, groups of isolated houses, skiing resorts and tourist resorts, as well as access networks. The access networks consist of short wireless links connecting together fixed end-users located in the same area and a set of hot-spots through which both fixed and nomadic users can access the network.

The gateway nodes to the Internet are usually located at the edges of one or more towns/villages. As we will see later, several gateways should be installed, in order to provide different routes to reach the Internet (i.e. the network should be multi-homed).

3. RELIABILITY AND QoS CONSIDERATIONS

3.1 Reliability considerations

In order to achieve reliability in ADHOCSYS networks, several aspects which affect reliability have been considered in our study. These aspects are node reliability, power supply reliability, software reliability and link reliability.

Node reliability may be affected by many factors. Particularly extreme weather conditions such as snow, wind, lightning, very low or very high temperature could lead to antennas bending, structural failures or misalignment with consequent degradation of link quality. The same weather conditions could cause electrostatic

discharges on network hardware or hardware working outside operating temperature range or short circuits due to water leakage or condensation inside the hardware. On the other hand rain and hail would not impair link quality because signal wavelength is not comparable to raindrop's size.

Power supply reliability may be affected by drained batteries and power outages. The problem of drained batteries may occur to nodes which are installed outdoors where AC supply is not available. The problem of sudden power outages caused e.g. by lightning has been addressed by trying to avoid them (through power supply redundancy), and by ensuring proper down and restart of the system in cases when power failures can not be avoided (through power watchdog). The network must be able to provide basic services even in case of power outages.

Software reliability involves the ability to deal with unexpected situations such as sudden cold restart due to temporary power outages or partial hardware damages. The software should continuously analyze node performance, compare it with baselines and send alerts to prevent node failures or battery outage. Software must be robust and should provide a quick and easy way to fix vulnerabilities.

Link reliability may be affected by the instability of wireless channels itself. Other factors such as weather condition, interference etc may also have influence on link reliability of certain paths. To provide non-interrupted services to end-users, reliable routing mechanisms are required so that an end-to-end path is still available even if there is a link break along the routing path.

3.2 QoS considerations

ADHOCSYS project is aimed in first instance at providing to all end-users an essential set of services, which includes e-mail and web browsing. High level services, such as high quality video streaming, IP Telephony and emergency calls, may be provided under specific conditions, depending on particular ADHOCSYS application scenarios. Providing consistent service differentiation and deterministic QoS, however, is a challenging task in all wireless networks. This is mainly due to the nature of the wireless communication medium and due to the characteristics of the CSMA/CA protocol for channel access used by devices compliant to the 802.11 standard [9].

To overcome these problems, the IEEE 802.11e TG has standardized an enhanced MAC protocol, aiming at providing mechanisms for service differentiation [10]. The Wi-Fi Alliance, on the other hand, defined a specification for the implementation of a subset of the draft 802.11e standard supplement, the so-called Wireless Multimedia (WMM). This choice "… is motivated by the need to prevent market fragmentation caused by multiple, non-interoperable pre-standard subsets of the draft 802.11e standard that would otherwise occur", according to [11]. This subset of the 802.11e standard, currently implemented in many commercial products, is illustrated in Figure 2. WMM is supported by the wireless devices used in the ADHOCSYS nodes (Wistron™ CM-9). The wireless drivers chosen for ADHOCSYS nodes [12] fully support the WMM specifications as well.

The main drawback of the WMM mechanism is that high efficiency levels in channel utilization are achieved only when it is configured to work in a probabilistic way (soft QoS). In other words, WMM does not offer hard guarantee for service differentiation. Different configurations of WMM, aimed at providing deterministic QoS (hard QoS), can dramatically reduce the overall efficiency in channel utilization.

Nevertheless, deterministic QoS can still be provided by using the QoS features of the Linux Kernel[1]. By using software level (Linux) queueing mechanisms, queue parameters can be set in order to provide deterministic QoS. The Hierarchical Token Bucket (HTB) mechanism [16], as part of the Linux Kernel, is implemented in each ADHOCSYS node and manages the node outbound policy. HTB has currently been used in many solutions, as both open source and commercial product. HTB is normally used for service differentiation in wired networks, but can successfully be used also for guaranteeing hard QoS in wireless networks. For instance, it has been used for wireless access during the PyCon 2007 conference, held in Dallas [17]. Its accuracy has been evaluated with extensive performance tests [18]. Commercial solutions already exist which implement HTB in order to guarantee accurate traffic shaping [18]. More related to our work, it has also been reported to successfully work in conjunction with WMM [19]. In ADHOCSYS networks, HTB will be employed in order to guarantee service differentiation within an ADHOCSYS node, while WMM will perform flow prioritization among different nodes.

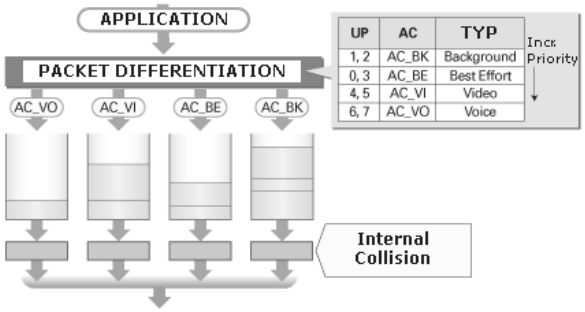

Figure 2. Representation of a subset of the 802.11e MAC.

To guarantee interworking between HTB and WMM queueing, classification of the various application types within ADHOCSYS is needed. Each information element (data packet) is classified via a unique IP Type of Service (TOS) value. Such objective is reached by using an open source suite for flow identification and classification which works at the application layer [13]. No modification to L1 and L2 standards is required, since the tagging is done at L3 (TOS field of the IPv4 header). Similar mechanisms (using 802.1Q VLAN tags) have been considered in [15].

Figure 3 shows the mechanism for packet tagging which has been implemented in ADHOCSYS nodes. When an ADHOCSYS node receives a packet, its source is checked. If an incoming packet comes from an external source (Internet gateway, users attached to the ADHOCSYS network), it is analyzed and classified (tagged) by the chosen traffic classification software. This mechanism can be computationally intensive if it is run on all nodes. In a stable ADHOCSYS network, however, the classification is made at the gateway when the packet enters the ADHOCSYS core network.

[1] Software installed in ADHOCSYS nodes is based on the OpenWRT distribution (URL: http://openwrt.org/).

Therefore, the likelihood that a non-classified (non-tagged) packet enters the ADHOCSYS network (grey dotted line in the following figure) has been kept very low.

As depicted in Figure 3, each packet of a given flow is tagged, depending on which application class the flow belongs to. Applications have been classified based on their QoS requirements:

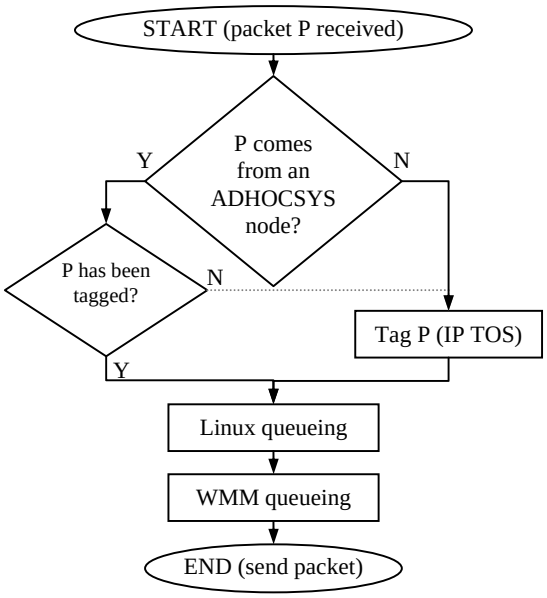

Figure 3. Packet classification in ADHOCSYS nodes.

- *Class I:* corresponds to applications which have strong latency constraints and small bandwidth such as Voice over IP and chatting applications (jabber, Yahoo! Messenger, etc.).
- *Class II:* is suitable for applications requiring high throughput such as transaction-processing applications.
- *Class III:* corresponds to interactive and best-effort type applications like web-browsing and e-mail.
- *Class IV:* corresponds to routing and battery information.
- *Class V:* corresponds to emergency calls.
- *Class VI:* corresponds to high throughput and latency constraint such as streaming video.
- *Class VII:* corresponds to peer-to-peer (P2P) applications.
- *Class VIII:* corresponds to unclassified traffic.

The above QoS definition for application Classes I, II, III is based on the conventional QoS classification which relies mainly on delay tolerance of different service classes. Classes from IV to VII have been defined in order to allow finer service differentiation policies.

To better exploit the functionalities of the HTB mechanism, these application classes have been further categorized into three application categories. Essential services for both users and networks are inserted in Category A. Category B groups flows with strict delay constraints, while Category C groups high throughput (but not essential) applications and uncategorized flows. Table 1 shows the mapping between application categories, application classes and WMM Access Categories (ACs). Figure 4 shows in more details the service differentiation mechanism in the HTB tree.

Table 1. Mapping between application classes, application categories and WMM Access Categories.

Category	Class	WMM AC
C	II, VII, VIII	0 (Best Effort)
B	I, VI	1
A	III	2
A, B	IV, V	3 (Highest Priority)

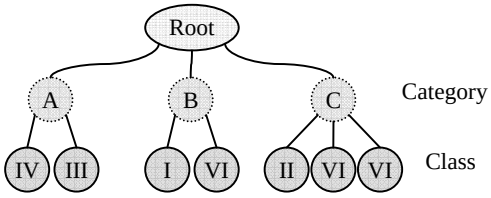

Figure 4. Structure of the HTB tree.

It is worth mentioning that one major difference with our QoS class definition, compared with the conventional QoS definition, is related to the different treatment for high bandwidth-demanding multimedia applications. While the conventional QoS vision puts this kind of traffic in the second highest priority class, that is, AC 2 (corresponding to AC_VI class in the vision of 802.11e/WMM), we allocate this traffic typology to the best effort class (AC 1). In other words, while the conventional QoS definition focuses solely on delay sensitivity of an application, we have further considered bandwidth requirement of an application, in addition to its delay sensitivity, in our traffic class definition.

Note also that our QoS definition is not node-based, but flow-based, which means that the traffic flows generated or received by a node may belong to different classes, as time varies. Therefore, for QoS class priority definition, the precedence has been given to traffic flows belonging to application Class III services, in normal conditions. When emergency calls occur, nevertheless, priority will be given to Class V traffic. Other QoS mechanisms which have been implemented in ADHOCSYS include link capacity and traffic load measurement and per-flow CAC. Please refer to [3] for more details.

4. RELIABILITY ANALYSIS AND AVAILABILITY PREDICTION

4.1 Reliability analysis

In order to obtain network reliability, redundancy is introduced at various levels. Redundancy significantly increases system reliability, and is often the only viable means of achieving reliability. However, redundancy leads to higher cost, and is therefore restricted to critical parts of the system. A quantitative reliability and availability prediction is useful to estimate quality assessment and resource planning (please refer to [6] for details of relevant theory).

From a reliability point of view, the ADHOCSYS network can be considered as a complex system, constituting several sub-systems such as nodes, links and Internet gateways, which as a whole must deliver a reliable service to the end-users. Each sub-system contributes to overall reliability of the system and their reliability

measurement is possible with the evaluation of particular parameters, such as Mean Time Between Failure (MTBF), a common reliability parameter used for instance also in electronic equipments, and Mean Time to First Failure (MTFF). Based on obtained parameters for these sub-systems, the reliability and availability of the entire system can be correspondingly predicted.

In ADHOCSYS, we propose a model to predict availability in order to ensure that the reliability requirement is satisfied for a given network configuration. More specifically, given an expected reliability for each node and link, we calculate the expected availability of the network, in order to identify how many redundant nodes or channels are required in order to serve a given number of users with high enough availability.

4.2 The reliability block diagram approach

Research work on network reliability analysis is traditionally based on wired networks. Popular analytical models include combinatorial methods, state-based methods, etc [4].

After considering the characteristics of all of these approaches, we decide to adopt the Reliability Block Diagram (RBD) model as the ADHOCSYS approach for reliability prediction. Although the method has not been explicitly designed for modeling wireless networks, it can be adapted to our case. The RBD based prediction can be performed according to the following three steps:

1) RBD modeling: All items involved in providing the network connection to a generic end-user must be put into a graph in which series entities represent the items necessary for the system to work and the parallel entities represent redundancies. Every item used into this representation can be in turn split into a lower level RBD.

Looking at Figure 5 which depicts a generic ADHOCSYS node RBD, we can see that all involved items are put into a series configuration (because all of them are required for the node to work) and the backup power items which are in a parallel configuration with respect to the main power ones.

The Routerboard (the core entity of our equipment) shown in Figure 5 is usually equipped with two network interface cards and two antennas: one for communication with other access points and one for connections with clients within its coverage. This means that both interfaces are needed at the same time and for this reason they are also put in series in the RBD.

2) Failure rates: The second step to achieve a system reliability and availability prediction is to identify to each building block of our system a failure rate. These data can be obtained mainly from three sources: in the most favorable cases the item manufacturer declares a failure rate. Otherwise one can rely on failure rate of equipment similar to the one used. The third chance is to perform some field evaluation as we did for wireless link behavior estimate.

Failure rate can be reported in various forms. The most common for electronic equipment is the MTBF expressed in hours. We will use also another form that is the Failure In Time (FIT) expressed in number of failures over a 10^9 hours period.

3) RBD reduction: This last step consists into a progressive simplification of the system level RBD when applying calculations derived from reliability theory.

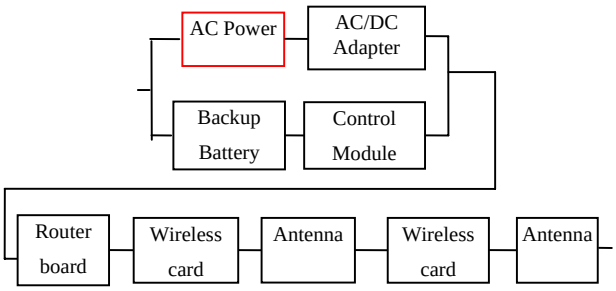

Figure 5. Generic ADHOCSYS node with backup power and two wireless cards/antennas used for connection to different nodes (series configuration).

A fundamental assumption for the analytical work presented hereafter is that failure rates (λ) are constant in time, which means that the failure probability of a given entity at a certain time is the same regardless how long it has been kept working in the past. This leads to an exponential failure distribution and, particularly the probability that an equipment is working at a given time, *R(t)*, can be expressed in the following formula:

$$R(t) = e^{-\lambda t} \qquad (1)$$

In this way, if we consider a series system of two items, like the one depicted in Figure 6.a), the probability that the system is working at a given time can be obtained in the following formula:

$$R_S(t) = R_1(t) \cdot R_2(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} = e^{-(\lambda_1+\lambda_2)t} \qquad (2)$$

And therefore:

$$\lambda_S = \lambda_1 + \lambda_2 \qquad (3)$$

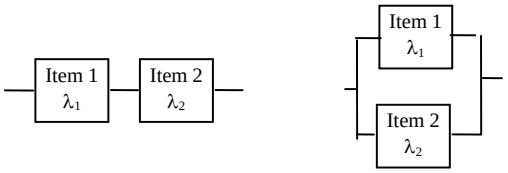

Figure 6. a) Series RBD (no redundancy); b) Parallel RBD (one redundant branch).

Similarly for the case of Figure 6.b) in which we have a parallel configuration i.e. one redundant path the resulting failure rate is expressed as:

$$\lambda_S = \lambda_1 \cdot \lambda_2 \qquad (4)$$

4.3 Network Availability

Availability is the amount of time a system is in working condition with respect to total amount of time elapsed and is an important parameter to assess if a service is at toll quality. The Availability of an entity can simply be computed in the following way:

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (5)$$

where the Mean Time To Repair (MTTR) is the time taken to repair the failed equipment. In our case we will have software failures that will cause automatic software restart (with a negligible MTTR) and hardware failures that will imply the replacement of

the involved equipment for which we can estimate an MTTR of 48 hours.

5. RELIABILITY CASE STUDY AND NUMERICAL RESULTS

In this section, we apply the reliability analysis and availability model presented above to a few cases and present the numerical results for these cases.

5.1 Nodes and Network RBD

The RBD at the network level will have the above described nodes RBD among its constituting blocks. Other blocks such as power supply and wireless links are also considered in this section.

The node power supply will be constituted by an AC source with relevant power adapter and by a backup source constituted by a battery and control module. These last items are considered in parallel for the RBD purposes.

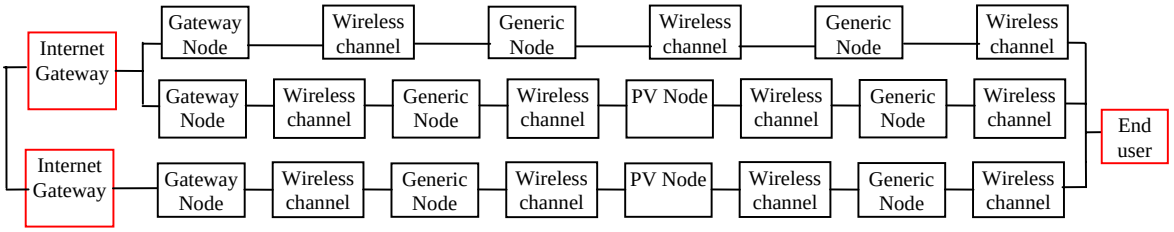

Figure 7. Best scenario: 3 paths to the end user and multi-homing with 2 Internet Gateways.

There are other possible node configurations that will lead to slightly different RBDs. In particular we can identify such cases as: Gateway Nodes with only one wireless Network Card and Antenna; and Photo Voltaic Nodes with a solar panel as the main power source and a Battery is needed for operation in night / overcast conditions which require all components in series, leading to worst reliability values.

5.2 Redundancy Scenarios

In this study we are interested in evaluating trade-offs between service availability and costs. For this reason we have proposed several scenarios in which the end-users are served by different amount of redundant paths.

In the following, we describe a few cases in order to further investigate the trade-offs, starting from the most complicated scenario discussed in [3], as illustrated in Figure 7. The other ones are progressively simpler and will be described briefly as follows.

1) Best scenario: In this case (Figure 7) an ordinary end-user is reached by 3 redundant paths, via two gateways. The main one is a 3-hop path that provides the fastest connection to the gateway. The second path is similar to the first one but with 4 hops, while the last one makes use of a Photo Voltaic Node. This implies the connection with a nearby no line-of- sight valley with available multi-homing.
2) One short and one long path: In this case there is a main path similar to the one of Scenario 1 and one redundant path with 8 hops, PV nodes and multi-homing.
3) Typical scenario without multi-homing: In this case we have the main path with 3 hops and one redundant path with 4 hops. There is only 1 gateway (multi-homing not available).
4) Worst scenario: In this case we have one path (with 3 hops) and no multi-homing.

One important assumption used in this work is that an ADHOCSYS network will be dimensioned for providing multi-media services (delay constrained services) but that, via a custom QoS implementation, precedence will be given to services that are less demanding in terms of throughput and real-timeliness such as web browsing and e-mail (delay tolerant services). In this way the 3 alternative paths of Figure 7 can be considered complete redundancy only for delay tolerant services and similarly the second path of Scenario 2) would not work for delay constrained services due to too many hops.

5.3 Failure Rate Prediction

To further pursue the analysis, the failure rates for each element of the RBD are needed. These elements include antennas, cables, connectors, Routerboards, wireless cards, power source, Internet gateways and wireless channels. As mentioned earlier, these values in our study are either obtained directly from manufacturer data sheet, or derived from similar hardware data sheet. The failure rate for wireless links is obtained through a real-life test network installed by ADHOCSYS project partners, which gave us a result of 99.6% availability (i.e. about 6 minutes of channel unavailability each day). More concrete values about failure rates can be found in [3] and [8].

5.4 Numerical Results and Discussions

Table 2 reports the availability results obtained for the various scenarios described in Subsection 5.2 of this section. Afterwards each scenario is briefly discussed.

Table 2. Availability results.

Block	Availability [%]	Availability [Nines]
Best scenario	99.997	5
One short and one long path	99.89	3
Typical scenario w/o multi-homing	99.87	3
Worst scenario	98	2

1) Best scenario: This scenario delivers a 5-nines availability such as the one that most end-users associate with well established fixed services with AC power and traditional telephony. Probably the costs involved in providing such a high level of redundancy are not justifiable.
2) One short and one long path: 3-nines of availability would probably satisfy most users for a wireless service in a rural area. Possibly this is the best scenario for what concerns availability/costs ratio and it should be easier to implement than the previous one.

3) Typical scenario without multi-homing: If a suitable level of redundancy is implemented in an isolated ADHOCSYS network, it can be achieved with an acceptable availability even without multi-homing.
4) Worst scenario: No redundancy and no multi-homing lead to very poor reliability performances (almost 6 days a year in terms of unavailability).

6. CONCLUSIONS

In this paper, we have presented a pragmatic and cost-effective solution for providing broadband Internet access in rural and mountain regions which is based on multi-hop wireless networks. Two aspects for designing such a network i.e. reliability prediction and QoS provisioning have been described in details.

More specifically, the presented model for predicting the availability of a multi-hop wireless network can be used in various phases of the network design. For example, to evaluate, in the network design phase, the best strategies to provide reliability through redundancy; to evaluate the achievable service availability versus the hardware and installation costs; to estimate the future maintenance costs; and to assess the advantages to provide fewer, more reliable pieces of hardware versus a larger number of cheaper ones.

The presented QoS mechanisms adopt a pragmatic approach which takes both delay sensitivity and bandwidth requirements into consideration for traffic class classification, in order to ensure an essential set of services with user satisfaction to all end-users while maximizing network resource utilization.

Currently, a pilot real-life network based on the presented approaches, together with other design aspects which are not included in this paper, is being deployed in Northern Italy.

7. ACKNOWLEDGMENTS

The work presented in this paper is funded by the European Commission through the FP6 IST STREP Project ADHOCSYS – Wireless Ad Hoc Broadband Monitoring System (No. IST-2004-026548). We wish to acknowledge the European Commission for their support. The authors would also like to thank all ADHOCSYS partners for their co-operation and contribution in this project.

8. REFERENCES

[1] F. Y. Li, L. Vandoni, G. Zicca, S. Zanoli, L. Leschiutta. Providing Reliable Internet Access with High Availability in Rural and Mountain Regions: An Approach via Multi-hop Wireless Ad Hoc Networks. *Broadband Europe Conference* (Geneva, Switzerland, Dec. 2006).

[2] L. Leschiutta, F. Volpi (eds.), P. Bucciol, A. R. Meo, S. Zanoli, O. Lazaro, F. Zubillaga, M. Di Girolamo, L. Vandoni, G. Zicca, F. Y. Li, M. Hauge, F. Pagliazzo, M. Ravalli. Specification of Detailed Requirements for Ad-hoc Network. ADHOCSYS project, Deliverable D4, IST-2004-026548, May 2006, available at http://www.adhocsys.org.

[3] L. Leschiutta (ed.), P. Bucciol, J. C. De Martin, L. Vandoni, G. Zicca, G. M. Giani, M. Giulini, F. Y. Li, S. Zanoli, F. Pagliazzo, M. Ravalli, V. Cristina, M. Mihaljevic, O. Lazaro, P. Sanchez. Specification of Algorithms for Static Reconfiguration of Ad-Hoc Network, and Multimedia Services, final version. ADHOCSYS project, Deliverable D14, IST-2004-026548, project restricted, delivered to the EC, May. 2007

[4] A. Jajszczyk (ed.), et al. . Description of Reliability Models of Resilient Networks. IST FP6 Euro-NGI Network of Excellence project (Sept. 2005).
URL: http://eurongi.enst.fr/archive/127/D.JRA.3.3.3.pdf.

[5] S. Maza, O. Lazaro, N. Cunha, L. Vandoni, and F. Y. Li. Broadband Access via Ad Hoc Networks: a Solution for Rural and Mountain Regions. *Broadband Europe Conference* (Bordeaux, France, Dec. 2005).

[6] P.D.T. O'Connor. Practical Reliability Engineering. Wiley, Chichester, England, 2002.

[7] ADHOCSYS web site. URL: http://www.adhocsys.org.

[8] L. Leschiutta, G. Zicca, F. Y. Li, L. Vandoni, and N. Fragoulis. Achieving Reliability via Multi-Homing and Path Redundancy in Multi-hop Wireless Networks for Internet Access in Rural Areas. *16th IST Mobile and Wireless Communications Summit* (Budapest, Hungary, 1-5 July 2007) (accepted for publication).

[9] ISO/IEEC 8802-11. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. ANSI/IEEE Std 802.11, 1999.

[10] IEEE 802 Committee. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - Amendment 8: Medium access control (MAC) quality of service enhancements. IEEE Std 802.11e, September 2005.

[11] Wi-Fi alliance. Support for multimedia application with quality of service in Wi-Fi networks.
URL: http://www.wi-fi.org, Sept. 2004.

[12] MadWiFi wireless drivers. URL: http://www.madwifi.org.

[13] P. Wang, H. Jiang and W. Zhuang. Capacity Improvement and Analysis for Voice/Data Traffic over WLAN. *IEEE Transactions on Wireless Communications* (to appear).

[14] Application Layer Packet Classifier for Linux (l7-filter). Available at http://l7-filter.sourceforge-net/.

[15] H. Zhu, M. Li, I. Chlamtac and B. Prabhakaran. A Survey of Quality of Service in IEEE 802.11 Networks. *IEEE Wireless Communications*, Aug. 2004.

[16] M. Devera. Hierarchical token bucket theory. URL: http://luxik.cdi.cz/~devik/qos/htb/manual/theory.htm.

[17] PyCon wireless network. Available at http://www.tummy.com/Community/Articles/pycon2007-network/.

[18] D. Ivancic, N. Hadjina and D. Basch. Analysis of precision of the HTB packet scheduler. In *Proc. 18th International Conference on Applied Electromagnetics and Communications* (ICECom 2005).

[19] Arcturus Networks, SIPjack(tm) series. Available at http://www.arcturusnetworks.com

[20] T. Sprull and J. Lockwood. Extensible Network Configuration and Communication Framework. Available at http://www.arl.wustl.edu/~todd/sproull_iwan_05.pdf