Wireless Self-Organizing Backbone Mesh Network (WiSoNet)

Heiko Kopp, Martin Krohn, Robil Daher and Djamshid Tavangarian

University of Rostock
Institute of Computer Science
Chair of Computer Architecture
E-mail: [firstname.lastname]@uni-rostock.de

Abstract

Despite significant advances in parts of the physical layer, available WLAN systems still cannot offer wired equivalent bandwidth. In this paper we propose a novel concept, called Wireless Self-Organizing Backbone Mesh Network (WiSoNet), for a wireless network infrastructure as a backbone and describe its long-term potential. WiSoNet combines two major IEEE Standards – IEEE 802.11 (WLAN) and IEEE 802.16 (WiMAX) to build a heterogeneous wireless network topology. To aggregate bandwidth of multiple WLAN connections we introduce a hybrid network solution that uses ad-hoc mechanisms. Further, to decrease the amount of administration and resource management, we use specific algorithms for the self-organization of routing and channels assignment. Since the WiMAX-based supply network already supports quality of service, we propose mechanisms to extend the QoS to end-users. Accordingly, we present our prototypical system implementation and discuss the issues we will focus on in the future.

1 Introduction

The Internet as one of the most exciting technical revolutions in the last century will remain the most efficient means of knowledge distribution in the future. The fast development of new broadband telecommunication services, like video and voice makes upgrading and enhancing the access infrastructure for internet-based services very necessary. Hence, wireless solutions are affected by a great variety of technologies and standards. The users demand for high throughput as well as flexibility and mobility can therefore be provided by heterogeneous wireless network systems only.

In this paper we propose a concept, called Wireless Self-Organizing Backbone Mesh Network (WiSoNet), for a wireless network infrastructure as a backbone and describe its potential. WiSoNet combines two major IEEE Standards – IEEE 802.11 (WLAN) [11–13] and IEEE 802.16 (WiMAX) [15] to build a heterogeneous wireless network topology. In that combination, WLAN and WiMAX are used to create an infrastructure that provides Internet access for huge areas without the need of wired components. By integrating a mesh multi-hop ad-hoc topology into a backbone, we get several advantages like the possibility to easily extend the networks, raise its reliability by introducing redundant routing paths as well as applying mechanisms for self-organizing the network infrastructure, e. g., for channel assignment to decrease maintenance costs. We define self-organization as possibility for devices to (re-)configure and maintain themselves with a minimum human intervention.

The combination of WLAN and WiMAX allows to extend the low range of WLAN by using WiMAX as backhaul to bridge uncovered areas, where no backbone infrastructure is present. Additionally, users of WLAN equipment may continue using this devices without a needed change to a new technology. However, despite significant advances in the parts of the physical layer, today's WLAN still cannot offer the same level of supplied bandwith as their wired relations. The actual data throughput at 54 Mbps of IEEE 802.11g and 802.11a is almost halved when taking all the overheads like MAC contention, headers and acknowledges into account [17]. Moreover, link-level data rates tent to fall quickly when distance increases between transmitter and receiver. This problem in a multi-hop topology is further aggregated because of interference with adjacent nodes in the same or neighboring paths [17]. The IEEE 802.11b and 802.11g standards provide three and the 802.11a standard provides 12 non-overlapping frequency channels, which can be used simultaneously within a neighborhood. This increases the effective bandwidth of the wireless network substantively. While aggregation is relatively common in WLAN infrastructure networks, it has been rarely applied to ad-hoc networks. Our goal is to bring this feature into wireless mesh networks without applying proprietary MAC protocols, but with system software modifications only. A

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE

major advantage is that we are now able to use components off the shelf in our network. [11–13]

The realization of a hierarchical network that includes WLAN and WiMAX is driven be the need of technologies that fill the gap between proprietary wireless point-to-(multi)point technologies and the necessity to allow users connect to the network in best case without change of their equipment. Using a flat ad-hoc architecture will lead to networks which do not scale well, when the number of nodes becomes large [9].

In Section 2, our presentation covers related work for all major issues our network system has to deal with. It then continues with a description of the proposed architecture in Section 3, including used routing and channel assignment. Additionally, security issues regarding node authentication, authorization of user access and accounting are presented. After that, Section 4 focuses on our first prototype network and a pilot installation. Finally, we both conclude and give an insight in further work in Section 5.

2 Related Work

The approach of hybrid hierarchical networks is well known and several solutions exist. While many proposed topologies use either ad-hoc networks or infrastructure networks, there are even combinations of both [19]. Our goal is to provide a flexible and self-organizing network infrastructure that integrates devices off the shelf. Therefore, we use mechanisms like auto-configuration and transport layer security in both the backbone and the access network. To provide an optimal bandwidth distribution in our mesh backbone while decreasing the administrative effort to maintain the network nodes, we use techniques like an automatic channel assignment [21], dynamic auto-configuration as proposed in [3] as well as self-organizing [10]. As large ad-hoc based architectures can become complex concerning routing and security, efficient mechanisms for automatic distribution of channels need to be developed. A possible way to combine routing and channel distribution is named as the *Hyacinth-Algorithm* [20]; however, is optimized for work in backbone scenarios with major traffic paths between user and traditional backbones.

To maintain secure communication and network maintainance, security issues for both user-to-user communication and network management, mechanisms like the framework for authentication in hierarchical sensor networks [2] can be utilized; however, they have not been adopted to WLAN systems in an efficient way.

3 Architecture

In the following, we present the architecture of our hierarchical network called WiSoNet. We start by describing the topology and terminologies used in the network and continue with the description of the routing and load-balancing algorithms. We finish with security and quality of service issues.

3.1 The three-tier hierarchical network

The three-tier network consists of the following hierarchy levels as shown in Figure 1:

- The *Supply Network* establishes a connection between the WiSoNet and the traditional backbone – thus the Internet. It uses IEEE 802.16-2004 as point-to-(multi)point technology.
- The second tier – the *Mesh Backbone Network* consists of multi-channel ad-hoc nodes building a mesh structure. They are responsible for routing traffic between the user and the Supply Network, as well as for connecting users to each other, directly. We use the IEEE 802.11a standard in ad-hoc mode, whereas each node contains multiple interfaces.
- The Access Network as third tier is responsible for user-access to the WiSoNet by using IEEE 802.11g interfaces. Additionally, authentication and accounting for users is done here.

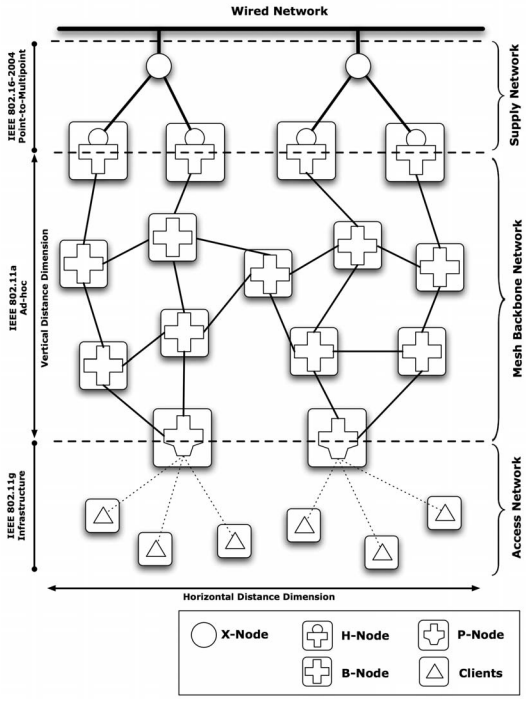

Figure 1. Components of the three-tier WiSoNet Architecture

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE

3.2 Components of the WiSoNet

Supply Network. The Supply Network as first of the three tiers in the WiSoNet Architecture takes advantage of the point-to-(multi)point technology WiMAX. We use components which are conformant to the IEEE 802.16-2004 standard [15]. They allow a maximum link-level throughput of 70 Mbps and operate within the 3.5 GHz frequency band. Although, the proposed range of a WiMAX base station is specified by around 50 km, current manufacturers state 20 km for Line-of-Sight (LOS) links as feasible. However, the denoted bandwith is directly proportional to the channel bandwidth, which itself is subject to local regulations. In Germany regulatory authorities limited the bandwidth of a channel to 7 MHz. This allows an overall bandwidth of 18 Mbps excluding management overhead. Our tests using currently available WiMAX equipment show that when deployed in a point-to-multi(point) scenario and with a LOS link, an average throughput of 4 Mbps in both directions over 1.5 km is possible. The Supply Network contains WiMAX Base Stations (called *X-Nodes* in Figure 1) and specially designed multi-technology nodes containing both WiMAX and WLAN interfaces. These interfaces act as bridges between both technologies. We call them *H-Nodes* and describe them in detail in the next paragraph.

Mesh Backbone Network. The second tier in our network hierarchy uses the IEEE 802.11a standard at 5 GHz to build a meshed WLAN ad-hoc network acting as a backbone network with redundant paths. The redundancy is used to aggregate traffic generated by the users of the network/ or arriving from the Internet by distributing packets over different paths. Within the second level we use multi-channel nodes – called *B-Nodes* – that contain multiple WLAN devices, where each node is responsible for maintaining direct links to as many neighboring nodes as possible. This leads to a highly dynamic topology even though our nodes are not concerned to be highly mobile. To achieve high performance in terms low maximum channel utilization, high throughput and low delay, we utilize the routing metric of interference and channel-switching (MIC) [22]. It improves the Weighted Cumulative Expected Transmission Time (WCETT) metric by providing an algorithm for an efficient algorithm to find loop-free minimum weight paths. We implemented this metric in our test pilot for nodes up to four interfaces and are currently investigating in performance evaluations regarding delay and throughput of flows and the overall load on the network.

Access Network. To provide connectivity to the network B-Nodes can be reconfigured to contain interfaces running in IEEE 802.11g master mode. Therefore, they become Access Point in an WLAN BSS infrastructure mode. These so called *P-Nodes* contain additional software components handling client authentication and authorization. This allows users to continue using their known wireless equipment when connecting to the WiSoNet. Additionally, we developed an embedded system in form of a DSL-modem that automatically configures itself to become a client within the WiSoNet. Therefore, users without wireless equipment can easily connect to the network without any configuration management.

3.3 Routing, Load-Balancing and Channel Assignment

As mentioned above, our Backbone Mesh Network as second tier uses ad-hoc mode, where each node is responsible for delivering data in the appropriate direction, either from the Supply Network to the clients, the clients to the Supply Network, or between clients. This routing is the mechanism that allows a node to decide where data has to be sent to reach its final destination. To comprise the multi-channel architecture we use within the backbone, special routing mechanisms are necessarily required, that consider all devices to determine the correct path of each packet.

There exist different types of routing protocols, each more or less adequate for wireless mesh networks. In our work, we rely on the Optimized Link State Routing Protocol (OLSR), a table driven, pro-active protocol that utilizes an optimization called Multipoint Relaying for control traffic. Modified to accomplish routing using multi-interface nodes and a routing metric called MIC, that takes interference between nodes and amount of channel switching into account, we provide a feasible system being robust yet performant.

A major task for us while developing the network architecture was the intention to provide automatic configuration of all nodes regarding their network parameter, e. g. used or unavailable channels. In your current implementation we utilize the Hyacinth algorithm [20] to provide distributed channel assignment. It uses local topology and local traffic load information to perform channel assignment and route computation. Unfortunately, it needs to share a common channel with all neighbors in communication range, which is subject for investigation in our further work.

All necessary information is collected from a $(k+1)$-hop neighborhood, where k is typically between 2 and 3.

Most of the traffic in the meshed network is send to or received from the Supply Network; hence, each B- or P-Node needs to discover a path to reach one H-Node. However, the H-Nodes can logically be considered as the root of a spanning tree, thus every B-Node will attempt to be a part of one or more of these trees. All spanning trees are connected to each other through the Supply Network. When a B-Node joins more than one spanning tree, it may dis-

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE

tributes its load and use them as alternative routes, e. g. in case links or nodes fail. The basic algorithm used to construct the routing tree is related to the IEEE 802.1d [16] spanning tree formation algorithm; its main differences are that the metric determining a parent is dynamic to achieve load balancing and a load-aware channel assignment technique is used to automatically form a tree where more relay bandwidth is available on links closer to the Supply Network.

3.4 Auto-configuration of Backbone Nodes

For easy deployment and adaption of the Backbone Mesh Networks all B-Nodes contain the ability to self-configure themselves within an existing network. To achieve a maximum degree of robustness, we designed the mesh network to work self-sufficient and to use self-organization techniques [10].

In case a new node is integrated into the network, a minimum default configuration is applied to it. This consists of a base pre-configured Service Set Identifier (SSID) and a certificate to authorize itself within the existing network. Therefore, large geographically and logical independend networks can be created. Further configuration parameters can be retrieved over the initially instantiated configuration link.

In respect to the WLAN architecture auto-configuration of nodes is performed in two steps. Firstly, the channel assignment is done using the Hyacinth algorithm mentioned above. This ensures a MAC-layer connection to neighboring nodes. Secondly, after associating channels, each device gets an IP-address by utilizing he Dynamic Host Configuration Protocol (DHCP) [7]. A device requesting integration into the network will broadcast an initial `DHCPDISCOVER` message. As the mesh structure of the Backbone Network does not allow automatic distribution of broadcasts, the corresponding neighbor node contains a DHCP relay server. The server takes care that the incoming discover message is transformed into a unicast and relays the message to the well-known DHCP server of the network. This obviates unnecessary flooding of the entire backbone with discover packets. While the assignment of the first interface is relatively simple, additional IP-addresses for further devices need to be discovered differently. The device randomly assigns itself an IP-address out of a dedicated address pool. This address is then propagated by the routing protocol and becomes available in the whole network thus allowing a direct communication between the device and the DHCP server. Now, the device is able to get its final IP-address.

3.5 Security Issues in Ad-hoc Networks

Within our hierarchical network, we consider different kinds of security mechanisms that have to be applied. The self-organization of our B-Nodes needs to be secure in terms of no faulty nodes accessing the resources of the network. Additionally, users need to authenticate themselves when accessing the network via P-Nodes. Generally, all network traffic needs to be protected against data theft or manipulation.

While the latter problem can be accomplished by implementing transport layer security as part of the IEEE 802.11i standard [14], authorization of nodes as well as authentication of users can be accomplished by Authentication, Authorization and Accounting solutions [8]. We are currently developing a system that allows applying transport layer security in terms of EAP/TLS [1] being used in ad-hoc based networks. Additionally a hierarchical accounting system based on RADIUS is implemented to achieve both, certificate based node authorization as well as user authentication. This includes authentication between H-Nodes, B-Nodes and P-Nodes as well as client and user authentication and authorization within the infrastructure networks provided by the P-Nodes. The successful authentication of the nodes within the Backbone Network authorizes each new node to become part of the backbone, thus rejecting malicious nodes. The client and the server generate a Pairwise Master Key (PMK), providing authentication against each other. This is followed by the IEEE 802.11i handshake phase to generate the encryption keys for transport layer security.

In important fact for security in wireless networks is the generated overhead which is a huge drawback when it comes to quality of service issues. Therefore, we do not use additional IP-layer security.

3.6 Quality of Service in WiSoNet

The resource ReSerVation Protocol (RSVP) [23] is designed to meet requirements of Integrated Service (IntServ) in multicast, heterogeneous IP network environment. However, the scarcity of bandwidth and high link error in WLAN (in ad-hoc and infrastructure mode) results that the direct apply of RSVP may lead to high overhead and unstable performance [18]. Further, the lack of cross-layer interactions between IP and MAC layers makes the static reservation processes of RSVP not adaptive to the dynamic nature of the wireless networks.

Due to the structure of the proposed WiSoNet, the related QoS-model must consider the QoS-issues in accordance with the nature (standards and structure) of each level of WiSoNet, i.e., different QoS-mechanisms are required for different levels. Further, the support of real time traffic,

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE

especially VoIP traffic, requires applying a kind of end-to-end QoS between the mobile clients on the one hand and the different kinds of nodes on the other hand. In that respect, a signaling gateway is required to enable the mapping between the different QoS-mechanisms on each X, H, and P-Node. In the following, we present our QoS-model for each level.

Access Network According to IEEE standards [11–13], the network connecting the APs of P-Nodes is considered as Distribution System (DS). The end-to-end QoS in this case can be applied on MAC or IP-layer, as proposed in a previous study [5]. The access points (AP) and STAs must be provided with the required components to negotiate the required resources. Moreover, the use of QoS-oriented load balancing mechanism [4] also enhances the QoS in the entire WiSoNet, especially in the access network. The combination of this structure and IEEE 802.11e on all APs and STAs should increase the provided QoS drastically [5]. However, the performance of these mechanisms is strongly dependent on the resource management on the related DS, i.e., QoS on the mesh backbone network.

Mesh Backbone Network Since this network represents an ad-hoc-based communication medium between APs in the access network and access routers (ARs) in the supply network, the lengths of routes between APs and ARs is held under certain threshold value to avoid large latencies and jitters, which could degrade the whole QoS in the WiSoNet. The selected routing protocols as well as the route balancing mechanisms are in the case essential for enabling a kind of controlled QoS. The QoS-mechanisms proposed in [5] enables a kind of resource reservation and admission control in the mesh WLAN network. The use of IEEE 802.11e should increase the provided QoS especially for real-time traffic, such VoIP traffic. However, the mesh WLAN network due to its ad-hoc nature forms the main challenge for applying end-to-end QoS in the proposed WiSoNet.

Supply Network The IEEE 802.16 [15] defines several MAC-based mechanisms (Service flow QoS scheduling, dynamic service establishment, and two-phase activation model) for providing end-to-end QoS between WiMAX-terminals, i.e., between X and H-nodes.

4 Prototype Implementation

To gain practical experiences with the WiSoNet and to determine feasibility, we built an eight-node prototype containing two H-Nodes, four B-Nodes and two P-Nodes. After testing this prototype we are currently installing it in a city area to gain practical results. In the following, hard-, and software components as well as initial results from the lab tests are provided. In the following, we will propose the hard-, and software components used within the nodes.

4.1 Hardware Components

The base for any kind of nodes is an Avila GW2348-4 Network Platform that utilizes an Intel XScale IXP425 processor with 533 MHz. It contains four type III Mini-PCI slots. Each H-Node contains three Winstron CM-9 WLAN 802.11a/b/g network cards, while B-Nodes and P-Nodes contain four of them. All cards use the Atheros-Chipset. While the H-Nodes and B-Nodes use IEEE 802.11a in ad-hoc mode, the P-Nodes have one device configured to operate in IEEE 802.11g master mode. As 802.11 interfaces operating at non-overlapped channels but mounted at the same device still interfere [6], we always use external antennas. Additionally, the channel assignment takes care that for devices operating at the same node, their channels are at least one channel apart from each other.

As WiMAX base stations in the Supply Network we use Redline AN-100 systems, that are compliant to IEEE 802.16-2004. In the current prototype the WiMAX SS is connected via Ethernet. Future versions shall use an integrated Mini-PCI WiMAX card.

4.2 Software Architecture

The software used within the network differs between the kinds of nodes. Common to all nodes is the use of an embedded Linux operating system. To drive the Winstron WLAN devices we use the madwifi-ng driver that allows master mode in combination with the hostapd for the P-Nodes and supports multiple devices.

The proposed route and channel assignment daemon modifies the routing tables of the operating system and assigns channels by the use of the Hyacinth algorithm. H- and B-Nodes use a special authentication daemon to provide authorization each other against neighbors while P-Nodes contain an additional authentication mechanism to authenticate clients and authorize users. All nodes allow building of secure transport layers as mentioned in Section 3.5.

4.3 First Results from the Lab-Test

After creating the network infrastructure in our lab, we made some initial tests for the WiMAX components. Using IxChariot, Version 6.3 by Ixia, we measured bandwidth, latency as well as the Voice-over-IP Mean Opinion Score (MOS) of the network for the WiMAX connection and the overall network containing the WLAN Backbone Mesh Network. The distance between Subscriber and Base-Station for WiMAX was 1.5 km. Utilizing a IxChariot basic

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE

test script simulating data transfer we measured an average throughput of 3.883 Mbps with a latency of 128 ms. Additionally, we applied a Voice-over-IP measurement leading to an average Mean Opinion Score of 4.35 (excellent quality).

In future work, we will present our results from the currently developed WiSoNet including both WiMAX and WLAN components. Additionally, simulations using the ns2 network simulator are part of our work.

5 Conclusion and Perspectives

Wireless networks based on WLAN systems currently remain limited in bandwidth and scalability, especially when compared to their wired counterpart. In this paper we introduced our novel concept for wireless networking utilizing two major wireless IEEE standards – WLAN and WiMAX. Both technologies have advantages in the proposed level of integration. While WLAN offers the ability to work in ad-hoc scenarios, WiMAX provides point-to-(multi)point connections with high throughput over long distances. In particular, this paper describes the architecture of a heterogeneous network and addresses several issues to be aware of, like routing algorithms, security, quality of service and maintenance. Hence, new combined protocols have been involved, like the proposed QoS mechanisms [4]. To allow self-organization in our ad-hoc network we currently focus on routing and load balancing by using the Hyacinth algorithm. However, because of the nature of the WiSoNet-Nodes, we are currently developing an advanced routing protocol that is able to create short routing paths between spanning trees in the network rather than having to send packets through the Supply Network. This leads to better quality of service when communication between clients in different parts of the network takes place.

References

[1] B. Adoba and D. Simon. *PPP EAP-TLS Authentication Protocol, RFC 2716*.

[2] M. Bohge and W. Trappe. An authentication framework for hierarchical ad hoc sensor networks. In *Proceedings of the 2003 ACM workshop on Wireless security*, pages 79–87. ACM Press, 2003.

[3] R. Campos and M. Ricardo. Dynamic autoconfiguration in 4g networks: problem statement and preliminary solution. In *Proceedings of the 1st ACM workshop on Dynamic Interconnection of networks*, pages 7–11, Cologne, Germany, 2005. ACM Press.

[4] R. Daher and D. Tavangarian. QoS-Oriented load balancing for wlans. In *The First International Workshop on Operator-assisted (Wireless Mesh) Community Networks 2006 (OpComm'06)*, Berlin, Germany, 2006.

[5] R. Daher and D. Tavangarian. Resource reservation and admission control in ieee 802.11 wlans. In *The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine 2006)*, Waterloo, Ontario, Canada, 2006.

[6] R. Draves, J. Padhye, and B. Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *Proceedings of the 10th anual international conference on Mobile computing and networking*, pages 114–128, Philadelphia, PA, USA, 2004. ACM Press.

[7] R. Droms. *Dynamic Host Configuration Protocol, RFC 2131*.

[8] L. Gommans, J. R. Vollbrecht, C. T. A. M. de Laat, G. M. Gross, and D. W. Spence. *Generic AAA architecture, RFC 2903*. IETF Internet Working Group, 2000.

[9] P. Gupta and P. R. Kumar. The capacity of wireless networks. In *Proceedings of the IEEE Transactions on Information Theory*, pages 910–917. IEEE Press, 2000.

[10] J. P. Hubaux, T. Gross, J. Y. L. Boudec, and M. Vetterli. Towards self-organized mobile ad hoc networks: the Terminodes project. *IEEE Communications Magazine*, 31(1):118–124, 2001.

[11] IEEE. IEEE 802.11a standard, 1999.

[12] IEEE. IEEE 802.11b standard, 1999.

[13] IEEE. IEEE 802.11g standard, 2003.

[14] IEEE. IEEE 802.11i standard, amendment 6: Medium access control (ma) security enhancements, 2004.

[15] IEEE. IEEE 802.16a standard, 2004.

[16] IEEE. IEEE 802.1d standard, media access control (mac) bridges, 2004.

[17] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qui. Impact of interference on multi-hop wireless network performance. In *Proceedings of the 9th annual international conference on Mobile computing and networking*, pages 66–80, San Diego, CA, USA, 2003. ACM Press.

[18] M. Li, B. Prabhakaran, and S. Sathyamurthy. On flow reservation and admission control for distributed scheduling strategies in ieee802.11 wireless lan. In *MSWiM'03*, 2003.

[19] M. J. Miller, W. D. List, and N. H. Vaidya. A hybrid network implementation to extend infrastructure reach. Technical report, University of Illinois at Urbana-Champaign, 2003.

[20] A. Raniwala and T. cker Chiueh. Architecture and algorithms for an ieee 802.11-based multi-channel wireless mesh network. In *Proceedings of the 24th Annual Conference of the IEEE – Infocom 2005*, 2005.

[21] A. Raniwala, K. Gopalan, and T. cker Chiueh. Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks. In *ACM SIGMOBILE Mobile Computing and Communications Review*, volume 8, pages 50–65. ACM Press, April 2004.

[22] Y. Yang, J. Wang, and R. Kravets. Interference-aware load balancing for multihop wireless networks. Technical Report UIUCDCS-R-2005-2526, Department of Computer Science, University of Illinois at Urbana-Champaign, 2005.

[23] L. Zhang, S. Berson, S. Herzog, and S. Jamin. *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification, RFC 2205*. IETF Internet Working Group, 1997.

Proceedings of the Fifth Annual IEEE International Conference
on Pervasive Computing and Communications Workshops(PerComW'07)
0-7695-2788-4/07 $20.00 © 2007 IEEE