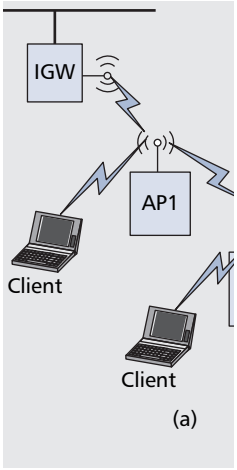
ACCEPTED FROM OPEN CALL

# WIRELESS MESH NETWORKS: CURRENT CHALLENGES AND FUTURE DIRECTIONS OF WEB-IN-THE-SKY

NAGESH NANDIRAJU, DEEPTI NANDIRAJU, LAKSHMI SANTHANAM, BING HE, JUNFANG WANG, AND DHARMA P. AGRAWAL, UNIVERSITY OF CINCINNATI




Wireless Mesh Networks offer an easy and economical alternative for providing broadband wireless internet connectivity and could be termed as the Web-in-the-sky.

## ABSTRACT

Within the short span of a decade, Wi-Fi hotspots have revolutionized Internet service provisioning. With the increasing popularity and rising demand for more public Wi-Fi hotspots, network service providers are facing a daunting task. Wi-Fi hotspots typically require extensive wired infrastructure to access the backhaul network, which is often expensive and time consuming to provide in such situations. Wireless mesh networks (WMNs) offer an easy and economical alternative for providing broadband wireless Internet connectivity and could be called the Web-in-the-sky. In place of an underlying wired backbone, a WMN forms a wireless backhaul network, thus obviating the need for extensive cabling. They are based on multihop communication paradigms that dynamically form a connected network. However, multihop wireless communication is severely plagued by many limitations such as low throughput and limited capacity. In this article we point out key challenges that are impeding the rapid progress of this upcoming technology. We systematically examine each layer of the network and discuss the feasibility of some state-of-the-art technologies/protocols for adequately addressing these challenges. We also provide broader and deeper insight to many other issues that are of paramount importance for the successful deployment and wider acceptance of WMNs.

## INTRODUCTION

The past few years have witnessed a tremendous growth of wireless LANs (WLANs) mainly due to their ease of deployment and maintenance. WLANs have been deployed in enterprises, universities, and public wireless hotspots, also known as Wi-Fi hotspots (airports, hotels, etc.) These Wi-Fi hotspots typically have one or more access points that are connected to the wired backbone network. Thus, deploying Wi-Fi hotspots requires extensive infrastructure and careful planning in order to minimize their costs.

Wireless mesh networks (WMNs) is an upcoming technology that envisages supplementing wired infrastructure with a wireless backbone for providing Internet connectivity to mobile nodes (MNs) or users in residential areas and offices, and could be called the Web-in-the-sky. WMNs are characterized by self-organizing self-configuring capability, ease, and (quick) rapidity of network deployment. Since its inception in the early years of this millennium, it has been in the limelight of all researchers. Massachusetts Institute of Technology's (MIT's) Roofnet [1, 2] and Microsoft's mesh networking project [3] are some efforts in this direction.

Unlike the traditional Wi-Fi networks, with each access point (AP) connected to the wired network, in WMNs only a subset of APs are required to be connected to the wired network. All the APs that are connected to the wired network are called Internet gateways (IGWs) or mesh points (MPs). APs that do not have wired connections, called mesh routers (MRs), connect to the MPs using the multihop communication paradigm. Similar to the wired network, where intermediate routers forward each other's traffic, in a WMN the MRs form the backhaul network and forward each other's traffic in order to establish and maintain their connectivity. Note here that MRs and MPs are similar in design, with the only exception that an MP is directly connected to a wired network, while an MR is not. Figure 1 shows a sample mesh network in a typical enterprise such as a university.

Many companies such as Nortel Networks, Strix Systems, and MeshDynamics are offering mesh networking solutions for building automation, small-scale and large-scale Internet connectivity, and so on using customary products. For instance, Strix systems have deployed 400 Strix MRs in an area of 100 km to realize a city-wide WMN in Tempe, Arizona, that would also provide voice over IP among other functionalities. Unfortunately, these companies often face tremendous challenges in designing, deploying, and ensuring optimal performance due to some inherent problems in multihop networks. Multi-


1536-1284/07/$20.00 © 2007 IEEE

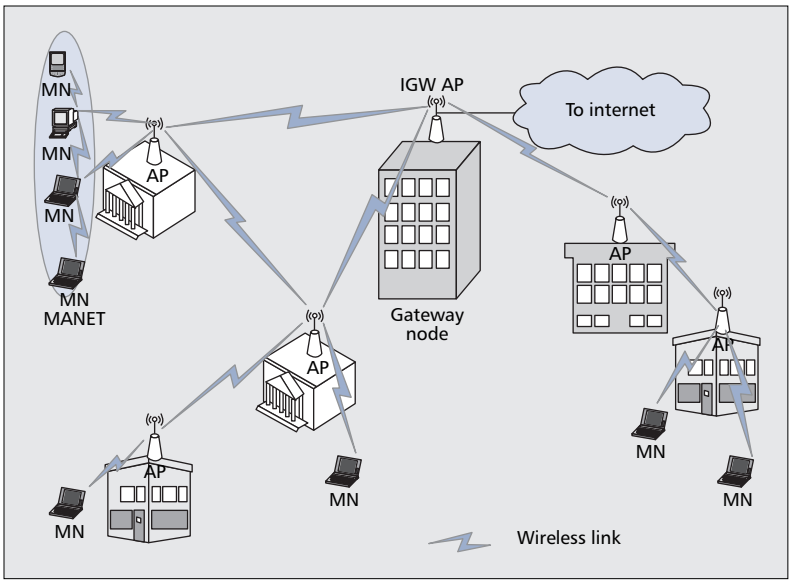



**Figure 1.** *A sample enterprise wireless mesh network.*

hop wireless communication is beset with several problems such as high interference, increased collisions due to hidden/exposed terminals, and high levels of congestion. In addition, effects of fading and shadowing lead to very unreliable link connectivity. Finally, all of them culminate in extremely low end-to-end throughput, which is highly undesirable in the perceived applications of WMNs.

Commercial interest in WMNs is prompting immediate and increasing attention to integrating them with the Internet. IEEE has set up many Task Groups such as 802.11s, for specifying the physical (PHY) and medium access control (MAC) layer standards. Specifically, the Task Group's target is to define an extended service set (ESS) that provides reliable connectivity and seamless security, and ensures interoperability of the devices. It proposes the use of layer 2 routing and forwarding. Industry giants such as Motorola Inc., Intel, and Nokia are actively participating in these meetings. Two main proposals from SEEMesh and the WiMesh Alliance were considered and successfully merged at the March 2006 meeting. The Task Group is actively working toward finalization of the standard and is expected to be approved by the end of 2008.

Although the envisioned applications of WMNs seem alluring, considerable work is still required at all communication layers before widescale deployment of these networks is practical. One of the key challenges is improving the capacity and guaranteeing minimum bandwidth. As mentioned earlier, providing broadband access for a community requires relatively higher bandwidth and various quality of service (QoS) provisions. However, current PHY/MAC/routing protocols cannot completely satisfy these requirements. These networks are expected to be self-configuring, self-healing, and resilient to device failures, and should be highly scalable. Thus, in order to succeed in the end user market, a systematic design approach at all layers is incumbent, and use of cross-layer information is inevitable.

The concept of mesh networking is very general and can be extended to different technologies. For instance, the IEEE 802.16 WiMax standard defines a mechanism for deploying a wide area wireless broadband network using a multihop mesh of powerful base stations. These base stations operate in licensed spectrum and have very long transmission range (around 70 mi). With the rapid progress in ultra-wideband (UWB) technology, short-range extremely high-bandwidth WMNs are also envisaged for indoor audio and video streaming applications. However, for the sake of clarity, in this article we focus on WLAN-based mesh networks. Akylidiz *et al.* [4] provide an overview of primitive mesh networks.

In this article we systematically examine the key challenges at each layer and discuss the feasibility of some approaches to address these challenges. Before we proceed to a detailed discussion of the various issues, we first enlist some of the unique features and characteristics that distinguish WMNs from existing mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs).

**Mesh routers are relatively static** — Therefore, the route selection should focus on discovering high-bandwidth links that could provide low end-to-end delay and interfere with as few nodes as possible, and should possibly exploit multiple path routes not only for resilience but also for load balancing [1].

**Mesh routers have no power constraint** — In contrast to traditional wireless networks (MANETs and WSNs) where nodes are typically power constrained, MRs have abundant power at their disposal. Hence, the MAC/routing protocols designed for MRs should primarily focus on maximizing the available channel bandwidth rather than on power constraints.

**Mesh routers are equipped with multiple radios** — With the plummeting costs of radios, MRs can now be equipped with multiple radios within the bounds of permissible form factor and inter-radio interference. We can thus accomplish simultaneous transmission and reception using intelligent channel assignment to these radios.

**Different traffic model** — Unlike MANETs where the traffic can be from any peer mobile node (MN) to any other MN, traffic in WMNs is predominantly between MRs and the IGW. MRs are used primarily as an intermediate hop to forward others' traffic.

**Traffic concentration may be higher along certain paths** — It may be valid to assume a uniform traffic distribution in MANETs, but in a WMN, traffic is primarily concentrated along the paths directed toward the IGW.

**Traffic volume and number of users** — As mentioned earlier, MANETs have been designed essentially for enabling communication within a small group of people. On the other hand, a WMN aims to provide high-bandwidth broadband connections to a large community and thus should be able to accommodate a large number of users accessing the Internet. In a WMN, the estimated traffic volume is very high, so scalability and load balancing in routing become important issues.

As there are considerable differences in the

architectural design and application scenarios between WMNs and MANETs/WSNs, we need to consider these unique features while designing protocols for WMNs.

## Physical Layer Issues

As the WMN is expected to provide broadband Internet access, it should have higher bandwidth. With the fast developments in very large-scale integration (VLSI) and digital communication technologies, the raw data rates that can be supported at the physical layer are rapidly increasing. Specifically, raw PHY rates have increased from 1 to 100 Mb/s (IEEE 802.11n [http://www.tgnsync.org/]) and soon may reach up to 1 Gb/s. However, these rates are only theoretically achievable, under perfect conditions with absolutely no interference. In real-world deployments, these idealistic conditions seldom exist. As the distance increases, the SNR decreases, as a result of which signals encoded using higher modulation techniques cannot be decoded at the receiver. With the ever increasing wireless devices in the market, interference from other sources can hardly be avoided. Thus, the theoretical data rates specified in the data sheets are not achievable in a practical scenario.

As a large number of nodes may exist in a WMN, interference also increases substantially. Clearly, the use of omnidirectional antennas severely reduces the achievable throughput due to interference. One alternative is to utilize multiple radios that can be operated on noninterfering channels. Another option is to use directional antennas. Recent developments in multiple input multiple output (MIMO) antenna technologies and smart antennas [5] can help in decoding wireless signals with low SNR, thereby increasing the achievable bandwidth. Moreover, using directional antennas to concentrate signal power in particular directions can help in better frequency reuse. Thus, use of such antennas at the physical layer can help cope with the growing interference that degrades the performance of wireless networks.

Although multiple radios can be used to significantly improve the throughput gains, improper placement may render them ineffective. Liese *et al.* [6] observed that if two antennae with a gain of 5 dBi are used in one access point (AP), a minimum separation of 3 ft is required in order to use noninterfering channels simultaneously. Moreover, if the antennae are placed too close to the ground, the signal strength degrades rather rapidly.

Power control is another interesting aspect that should be thoroughly investigated. Since the nodes in a WMN can be placed anywhere, topology control becomes important. Typically, assigning optimal power for controlling the topology can reduce interference and in turn help improve overall network performance. Having access to or control of parameters such as transmit power, modulation, and received signal strength at upper layers will help in optimizing the overall network performance. Cross-layer interaction is inevitable. Kawadia *et al.* [7] discuss various precautionary measures that should be considered while using a cross-layer approach.

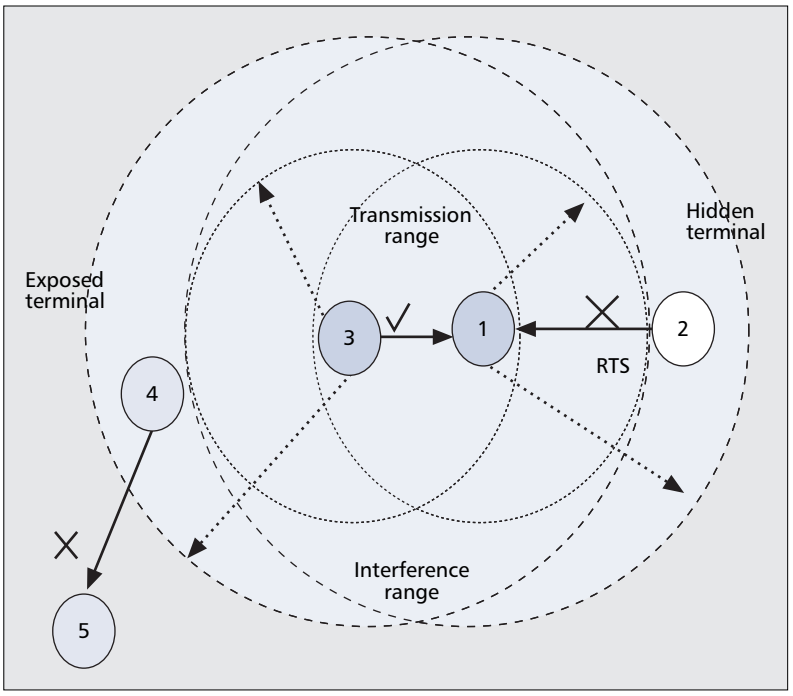



**Figure 2.** *The hidden and exposed terminal problems.*

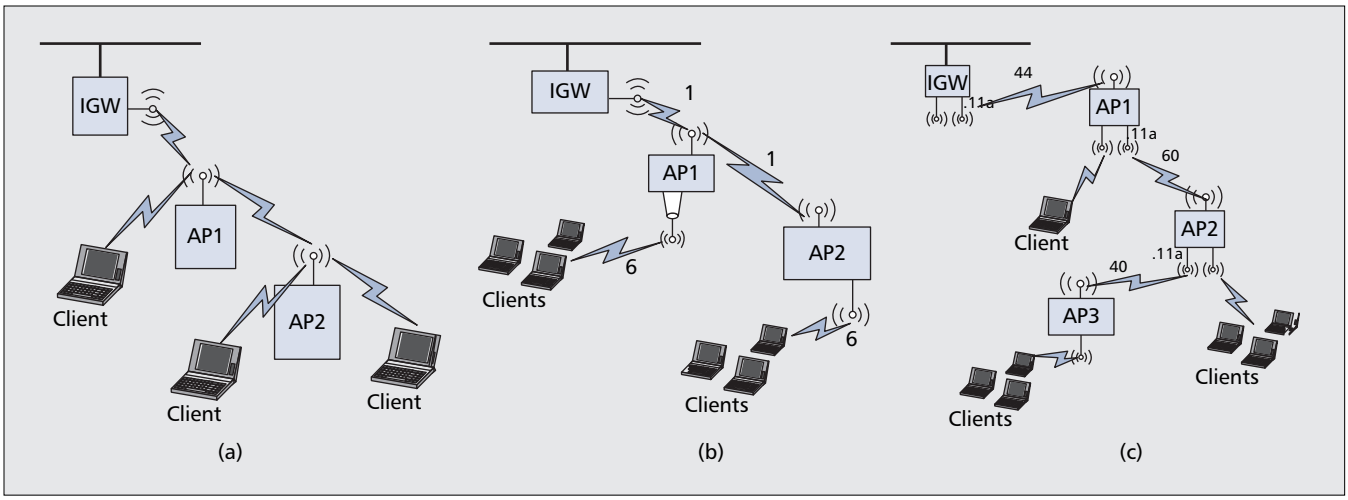
### *Open Research Issues*

- The number of noninterfering channels is finite and may be insufficient in some scenarios where the node density is high.
- The cost and complexity involved with such systems is high.
- A careful design of multichannel/directional systems needs to be considered so that the upper layer protocols are able to fully utilize their features.
- Cross-layer design should be prudently considered, as it may lead to complex system design that may be inflexible for future developments.

## Media Access Issues

Even though the PHY rates have considerably increased, current media access protocols are not able to realize the entire bandwidth provided by the PHY layers. The primary reason for this subdued performance is due to improper or suboptimal media access protocols that have been designed primarily for single-hop networks. For example, the widely accepted MAC protocol IEEE 802.11 DCF, when used in a multihop network, results in exiguous performance and is unacceptable. Some nodes may remain starved due to hidden and exposed terminals in a multihop environment. Figure 2 illustrates these problems. Node 2, which is outside the interference range of 3, is unaware of the ongoing transmission at node 3, and continues to send requests-to-send (RTS) to node 1, causing collision. This is called the hidden terminal problem. Node 4 is prevented from transmitting because of the neighboring transmission at node 3. This is called the exposed terminal problem. An ideal MAC protocol for WMNs should provide fair access to all nodes competing for the channel.

Prior research in MAC protocols in either




■ **Figure 3.** *a) Single-radio single-channel mesh network; b) dual-radio single-channel mesh network; c) multiradio multichannel mesh network.*

WSNs or MANETs has been primarily oriented toward energy conservation. However, for MRs, power is no longer a constraint, and the focus of MAC protocols should be on achieving higher throughput rather than energy conservation issues.

Even with an efficient MAC design, fairness among flows of different hop lengths may not be achieved [8]. In multihop networks, a packet has to be forwarded by many intermediate nodes. Whenever an intermediate node receives a packet for forwarding, it has to perform IP layer lookup and Address Resolution Protocol (ARP) lookup, and then contend for the channel at the MAC layer at each hop. This not only increases end-to-end delay, but also dramatically amplifies the probability of packet loss.

A single--radio single-channel mesh architecture is shown in Fig. 3a. Ramanathan *et al.* [9] suggests a radical change spanning across routing, MAC, and PHY layer protocols to speed up the process of forwarding in these networks. Assigning orthogonal channels to the MRs within the interference range can help alleviate the hidden and exposed terminal problems, and assist in improving the overall capacity of the network. So *et al.* [10] proposed multichannel MAC protocols using a single radio for ad hoc networks and showed the performance gains. But considering the traffic characteristics in a WMN, frequent channel switching may be required to communicate with neighboring nodes. In such scenarios, single-radio multichannel MAC may not provide any significant performance gains because of the high channel switching delay.[1] The plummeting cost of wireless radios has opened up new avenues for designing MRs using multiple radios. MRs can now use multiple radios tuned to orthogonal channels for simultaneously communicating with their neighbors. Figure 3b shows the use of a dual-radio WMN. One radio provides service to its mesh clients (using channel 6 in 2.4 GHz 802.11 b/g), and the other radio forms the backhaul link connecting all the MRs to the IGW (using 5 GHz 802.11a). However, it suffers from the disadvantage of sharing the bandwidth with the neighboring MRs at each hop along the backhaul link to the IGW.

Figure 3c shows the use of a multichannel approach using multiple radios that successfully overcomes all the problems encountered in the other architectures. Ideally, two radios are employed for the backhaul link and one for servicing the mesh clients. The uplink and downlink backhaul radios and the service radio are all operated at nonoverlapping channels, eliminating potential co-channel interference. As each mesh router can be equipped with multiple radios, fixed channel assignment to these radios is a more viable solution. Efficient and intelligent channel assignment schemes have to be designed as the number of channels is not infinite or may not be sufficient in a high node density scenario. Several channel assignment mechanisms [11–14] are being proposed. Elegant assignment schemes can also be derived from graph coloring approaches [15]. Ramachandran *et al.* [13] investigate the channel assignment problem based on an interference-estimation technique. Adya *et al.* [11] perform the channel assignment using a measurement-based approach that is dependent on channel quality for selecting the appropriate channel. Deafness is another key issue that has yet to be addressed in such an environment.

Many commercial MRs[2] currently in the market use multiple radios with multichannel capability for improving channel capacity. As all these vendors use their own proprietary MAC and routing protocols for their products, interoperability cannot be guaranteed. A multiradio unification protocol, a virtual MAC, proposed by Adya *et al.* [11] is an interesting approach to managing multiple radios. But concrete and robust native layer 2 protocols can be more effective and efficient than such virtual MAC solutions. With multiple radios communicating on noninterfering channels, an interesting aspect to focus on is efficient flow scheduling in a neighborhood so that resource usage can be maximized.

Another important issue that needs attention is QoS provisioning. The envisioned scenario of

[1] *In Atheros chipsets channel switching delay is close to 10 ms, which is considerably higher when we consider the transmission rates.*

[2] *Kiyon Inc. and, MeshDymanics are two of the startup companies actively involved in manufacturing commercial MRs.*

WMNs is expected to support applications like broadband Internet access, and real-time applications such as video streaming and voice conferencing. QoS provisioning for such key applications is an essential requirement and a key challenge. Performance of IEEE 802.11e (which was proposed for QoS provisioning in WLANs) over multihop networks is yet to be investigated. Therefore, existing MAC protocols have to be redesigned for efficient operation over WMNs. Thus, suitability of IEEE 802.11 MAC in a WMN is definitely debatable. A summary of some open research issues in the MAC layer are listed below:

***Open Research Issues***

- Intelligent channel assignment should be designed for efficient spectrum utilization among multiple radios.
- Innovative techniques should be implemented to convey the channel assignment of a node to its neighboring nodes.
- Scheduling of flows should be done intelligently for maximizing resource utilization.
- Support for different QoS levels in a multiradio multi-channel architecture using IEEE 802.11e should be investigated.

## Routing Issues in Mesh Networks

Existing routing protocols for multihop networks such as AODV and DSR are primarily designed for low-end MANETs and are inefficient for the WMN scenario [1]. The chief goal while designing routing protocols for MANETs and WSNs has been to conserve energy and improve packet delivery ratio. They are designed to search for stable routes in order to be robust and resilient to mobility. In these networks nodes are typically equipped with a single radio and share the same channel for communication with each other. As the channel is shared, choosing a route with a minimum number of hops is ideal for achieving better performance in MANETs. This is because a route with a smaller number of hops involves fewer forwarding nodes, and consequently fewer transmissions and less energy consumption. Furthermore, higher packet delivery ratios can be guaranteed with fewer hop routes in error-prone wireless channels. In contrast, MRs are neither power constrained nor highly mobile. Thus, the focus of routing protocols for WMNs should be on achieving higher throughput rather than saving energy or improving resiliency for mobility. Another key challenge in WMNs lies in identifying the best possible routes to the gateways from and to mesh clients. There are several other design considerations that require significant attention, which we discuss further in this subsection.

### Multirate Links

Ironically, minimum hop routing metric has very poor performance in a stationary multihop network [2]. Thus, when selecting paths in WMNs, instead of a hop-centric design, we need to consider throughput and an interference-centric approach. The primary reason for such poor performance in a static environment is the selection of suboptimal links (that are longer in range) which leads to higher packet loss and lower throughput. The link quality is affected by two factors: the distance between the transmitter and the receiver, and the interference at the receiver. Choosing a route with minimum hops results in selecting links that are further apart (i.e., the distance between the end nodes of the link increases). As the distance between the transmitter and receiver increases, the SNR correspondingly decreases. But a high SNR is required at the receiver for decoding packets transmitted at high PHY rates.[3] Thus, when packets are routed by a minimum-hop-centric method, packets transmitted at higher rates cannot be decoded, as a result of which packet error rate increases. In order to minimize packet error rate, nodes are forced to compromise for lower data rates, which results in lower aggragate throughput in the network.

DeCouto *et al.* [2] take link losses into account and present a performance metric based on expected transmission count (ETX) at each node to its next hop. ETX considers the forward and reverse drop probability of links and accordingly rates the path. However, it does not take the throughput of the links into account; thus, this metric may allow lower-throughput links.

### Multiple Radios, Multiple Channels Force Interaction between Routing and MAC Layers

As a WMN is likely to serve a large number of users, it requires high capacity. Using multiple orthogonal channels may be inevitable for achieving the required capacity. However, using multiple channels over a single radio can cause considerable delays, mainly due to channel switching latency and synchronization. This mitigates the true advantage of using multiple orthogonal channels. Fortunately, as the prices of wireless adapters keep dropping, it is economical to equip MRs with multiple radios. Each interface can be statically tuned to a different orthogonal channel, obviating the need for frequent channel switching. Intelligent channel assignment to these radios can greatly improve the capacity of the network. Alicherry *et al.* [16] propose heuristics for joint channel assignment, routing, and link scheduling for multiradio WMNs. They focus on achieving optimal channel assignment with an interference-free link schedule and routing by satisfying certain fairness, link congestion, and link scheduling constraints among others. However, with the introduction of multichannel multiradio architecture, the number of possible routing alternatives increases, and route selection becomes more complex. The routing algorithms should not only enable selection of high-throughput links with low end-to-end delay, but also ensure minimal interference between neighboring nodes. Interference is a critical issue in wireless networks. Estimating link interference is nontrivial and typically requires $O(n^4)$ comparisons for checking the interference between every pair of links in an $n$-node network. Padhye *et al.* [17] propose an empirical methodology for estimating the same that minimizes the comparisons to $O(n^2)$.

As a WMN is likely to serve large number of users, it requires high capacity. Using multiple orthogonal channels may be inevitable for achieving the required capacity. However, using multiple channels over a single radio can cause considerable delays, mainly due to channel switching latency and synchronization.

[3] *Packets transmitted at high PHY rates are encoded using complex modulation techniques and thus require high SNR at the receiver to decode them.*

Capacity is a key issue in WMNs. There are several elements that decide the capacity of WMN, such as network architecture, network topology, traffic pattern, network node density, number of channels, transmission power level, etc.

Even with this reduction, the time required for estimating remains very high, necessitating further improvement in the design of effective techniques.

### Impact of the Traffic Model

MANETs have been predominantly designed to facilitate sharing of network resources and data among a set of dynamic users. Typically, the traffic in a MANET is between any two nodes in the network. However, in WMNs the traffic is oriented either toward (upstream) or away from (downstream) the IGW. Also unlike MANETs, the expected traffic volume in WMNs is very high. The use of traditional routing protocols designed for MANETS in WMNs may lead to subdued performance due to the presence of hotspots near an IGW.

It is imperative for any routing protocol designed for WMNs to include efficient load balancing capabilities. It is also important to incorporate efficient search techniques to select the best among the multiple paths and employ efficient traffic splitting among these routes [1]. Multipath routing increases the reliability and robustness of the network. Existing literature on multipath routing in MANETs/WSNs primarily focuses on finding edge disjoint or node disjoint routes for energy efficiency. Although use of node disjoint routes may be feasible in a WMN, the use of maximal disjoint routes can yield better distribution of traffic load.

Another important issue is link stability. Due to varied reasons such as interference, fading, and shadowing, links are highly unstable. As a result, frequent route flaps occur, leading to an extremely unstable and unpredictable network. Thus, metrics designed for WMNs should be able to capture the link stability in the network.

Draves *et al.* [3] propose a new routing metric, Weighted Cumulative Expected Transmission Time (WCETT), for multiradio multichannel networks. They improve ETX by taking into consideration throughputs of the links and channel diversity. The proposed metric chooses routes having high throughput links (consequently lower end-to-end delay). Furthermore, they also consider intraflow interference (packets of the same flow contend with each other at different hops) and alleviate this by cleverly selecting routes that involve channel diversity. Although WCETT is shown to work well in a multiradio multichannel network, it has limitations due to interflow intereference that make it unsuitable for large networks.

Raniwala *et al.* [14] propose Hyacinth, a multichannel WMN in which each mesh node is equipped with multiple 802.11 network interface cards (NICs). They explore distributed channel assignment and routing by first creating a spanning tree rooted at the gateway. The available NICs are divided among the parent node (UP-NIC) and the children nodes (DOWN-NIC). The DOWN-NICs of the parent and the UP-NICs of the children are tuned to the same channel for communication, and the channel to be used is assigned by the parent. However, load-sensitive path metrics are not suitable or optimal for WMNs.

Ramachandran *et al.* [18] propose a spanning-tree-based protocol, AODV-ST, that modifies the popular AODV protocol by including expected transmission time (ETT) as the routing metric. In their work the mesh relays/routers construct a spanning tree corresponding to each gateway in the network. Each MR maintains a primary gateway (with the least end-to-end delay) and routes traffic through this gateway. Load balancing is achieved by prudently routing the traffic flows through the least loaded gateway. In order to estimate the least loaded gateway, periodic round-trip time (RTT) probing is performed. If the least loaded gateway found is not the default gateway, new traffic flows are routed through that node, and existing flows continue to use the earlier path. However, they do not consider routing in multichannel architecture, and inter- and intraflow interferences remain a big challenge.

In summary, while designing routing algorithms and metrics for WMNs, the following challenges should be addressed.

#### *Open Research Issues*

- Routing metrics should ensure that low-bandwidth links are seldom selected when links of higher bandwidth are possible.
- Routing metrics should incorporate link stability so that frequent route fluctuations can be avoided.
- Metrics should choose routes that have good channel diversity to minimize intra- and interflow interference.
- A routing algorithm should perform load balancing and ensure that a router does not become a bottleneck node.
- Any load balancing algorithm that is designed should have quick convergence and not be oscillatory. At the same time, it should allow good usage of network resources.
- Loop-free routing should be guaranteed.
- Routing algorithms should provide QoS guaranteed paths or at least some support for QoS provisioning.
- Efficient route recovery and maintenance should be provisioned.
- Elegant techniques to handle handoffs and minimize handoff latencies should be designed.

## Capacity Issues in WMNs

Capacity is a key issue in WMNs. In the past decade, several research efforts have been made to study the capacity of wireless ad hoc networks that can be adapted to the area of stationary multihop networks. These studies mainly focused on the issue of scalability of the throughput with the size of the network (i.e., the number of nodes $n$ in the network). There are several elements that decide the capacity of a WMN, such as network architecture, network topology, traffic pattern, network node density, number of channels, and transmission power level.

One of the seminal works was done by Gupta and Kumar [19], who analyzed the capacity of stationary wireless networks from the viewpoint of information theory. Their research is based on the principle that the interference between neighboring nodes utilizing the same channel to

transmit data is the reason for the constriction in capacity. When several nodes transmit simultaneously, a receiver can successfully receive the data sent by the desired sender only if such interference from local neighborhood is sufficiently small. In their model, they consider $n$ homogeneous nodes (with the same capability of transmitting data at $W$ b/s and the same radio range) that are randomly deployed. For each node, a destination node is randomly chosen. Based on the analysis on both the protocol and physical models, the following analytical lower and upper bounds of network capacity are derived: When the nodes are randomly deployed with random communication pattern, the throughput per source-destination pair is

$$\Theta\left(\frac{W}{\sqrt{n\log n}}\right),$$

while the throughput achieved is

$$\Theta\left(\frac{W}{\sqrt{n}}\right)$$

when node placement and communication pattern is optimal. From the analytical results, it follows that the throughput capacity per node reduces significantly when the node density increases. An important implication derived from [19] is regarded as a guideline to improve the capacity of ad hoc networks: A node should only communicate with nearby nodes. Another important conclusion is that dividing the channel into subchannels does not change the above capacity bounds.

By allowing the nodes to move, Grossglauser and Tse [20] showed that the per-user throughput can be increased dramatically. In their research, if node motion is independent across nodes and has a uniform stationary distribution, a constant throughput scaling $\Theta(1)$ per source-destination pair is feasible. This is obtained by exploiting the multi-user diversity benefits of having additional "routes" between a source and a destination.

Assuming the same physical model as in [19] but with a different traffic pattern (a relay traffic pattern), the network capacity is studied in [21]. In this model there is only one active source-destination pair, while all other nodes assist this transmission. Under two additional assumptions, they derive upper and lower bounds for the capacity using the max-flow min-cut theorem: When the number of nodes in the network goes to infinity, the asymptotic capacity is $O(\log n)$ b/s.

As discussed above in [19] and related publications, the throughput optimal schemes have been well studied, while the trade-off between the delay and throughput for such schemes has not received much attention. Based on the models studied in [19, 20], Gamal *et al.* [22] analyzed the delay and determined the throughput trade-off in both fixed and mobile ad hoc networks. For the Gupta-Kumar fixed network model, they showed that the optimal throughput-delay trade-off is given by $D(n) = \Theta(nT(n))$, where $T(n)$ and $D(n)$ are the throughput and delay, respectively. For the Grossglauser-Tse mobile network model [20], their results showed that the delay scales as $\Theta(n^{1/2}/v(n))$, where $v(n)$ is the velocity of the mobile nodes. In [22] they also designed a scheme that achieves the optimal order of the delay for any given throughput value. To achieve the optimal throughput-delay trade-off, the scheme varies several elements — the number of hops, the transmission range, and the degree of node mobility — to achieve the optimal trade-off. Both the Gupta-Kumar and Grossglauser-Tse models are included in this scheme as two extreme cases.

Due to the difference between WMNs and MANETs, analytical results of MANETs may not be directly used in WMNs. Jun *et al.* [23] considered the major difference between WMNs and ad hoc networks, which is the traffic pattern. Typically, traffic in WMNs is gateway oriented (i.e., either to or from a gateway), while in ad hoc networks the traffic flows between any arbitrary pair of nodes. Based on this special property of WMNs, they study the capacity from the chain topology and propose that for WMNs the throughput of each node decreases as $O(1/n)$. The reason for the poor performance of WMNs compared to pure MANETs is the fact that gateways are the hot spot of network traffic and could be a potential bottleneck of the whole network's capacity.

Another limitation of the existing research is that the focus has been on the theoretical analysis for the asymptotic case. Exact capacity analysis is another major contribution of [23]. For a given topology and number of active nodes, they provide exact upper bounds on the throughput of any node. Jain *et al.* [24] showed more research progress in obtaining the exact capacity of a multihop wireless network. Previous work focused on asymptotic capacity bounds always worked under the assumptions of homogeneity of nodes, and randomness of network topology and/or workload. However, they presented a model and a methodology for computing upper and lower bounds of the optimal throughput for the given network topology and workload. To achieve such optimal throughput, the nodes should have the ability to control and schedule packet transmissions according to requirements. Some optimal routes are found instead of the traditional shortest path routes. A conflict graph is then used to model wireless interference between neighboring nodes.

Recently, one approach has been discovered for increasing the network capacity of WMNs by employing multiple channels. Most existing research on wireless network capacity typically considered wireless networks with a single channel. Kyasanur *et al.* [25] derived the lower and upper bounds on the capacity of a static multi-channel wireless network. They study a wireless network model that has $c$ channels and $m \le c$ interfaces per node. They analyze the impact of the number of channels and interfaces per node on network capacity, and find that in an arbitrary network, if the number of interferences per node is smaller than the number of channels, there may be a loss in network capacity. An interesting result in a random network with up to $O(\log n)$ channels is that for each node, even with a single interface, there is no capacity

Though there exist several research solutions for the capacity problem for the ad hoc networks, considering the differences between WMNs and ad hoc networks, many open research issues still exist in adopting the solutions for WMNs.

A selfish node always acts alone and does not collude with others. In contrast, a malicious misbehaving node, with the intent to disrupt network activity by creating routing disruptions and possible network partitions, is more likely to collude with other misbehaving nodes.

degradation. They also studied the relationship between interface switching delay and network capacity. Their results show that in a random network with up to $O(\log n)$ channels, if each node is equipped with some extra interfaces, interface switching delay will have no impact on network capacity.

Although there are several research solutions to the capacity problem for ad hoc networks, considering the differences between WMNs and ad hoc networks outlined earlier, many open research issues still exist in adopting the solutions for WMNs. Some the challenges are outlined below.

#### *Open Research Issues*

- In order to increase the capacity and reliability of the network, new gateways can be added. A strategy to decide on the optimal placement of gateways should be designed.
- Cross-layer consideration may be used to improve network capacity.
- Optimal route selection strategies should be considered to increase the throughput of the network.

## SELFISH BEHAVIOR AND COOPERATION

The self-configuring and distributed nature of WMNs and the ease with which an MR or MP can be added makes it pertinent to ensure the secure operation of the network. It also paves the way for rogue nodes called free-riders that merely enjoy the network resources without contributing the needed functionality to the network. Furthermore, as the network can consist of nodes from different domains with conflicting interests, the nodes might not act cooperatively, and there is a high possibility of such free-riders. Naive assumptions that all nodes are cooperative in forwarding each other's packets impose serious threats to the secure operation of a network.

There is an important distinction between selfish and malicious nodes that should be noted. A selfish node would try its best to avoid detection, and these stealthy counter-attacks against detection have to be taken into account when designing a detection scheme. A selfish node, in general, is less motivated to get involved in collusion as it is greedy by principle in using the channel for itself. Acting so would be rather counterintuitive to its intentions. Hence, a selfish node always acts alone and does not collude with others. On the other hand, a malicious misbehaving node, with intent to disrupt network activity by creating routing disruptions and possible network partitions, is more likely to collude with other misbehaving nodes.

A selfish MP that provides access to other MRs might try to greedily consume the available bandwidth by favoring its own traffic and discretely dropping others'. This leads to a situation where the performance of certain flows can be in jeopardy. We term this selfish behavior *active selfishness*. Another possibility is that some MRs may refrain from advertising routes through them, thus proactively becoming selfish to maximize their bandwidth and economize their energy, consequently creating a network partition. We call such misbehavior *passive selfishness*. Thus, when designing routing protocols for these WMNs, an efficient methodology should be in place to carefully identify and punish such selfish MRs in the network. Detecting active and passive selfishness is one of the key challenges in ensuring secure operation of the network. Classifying an MR as selfish requires careful monitoring of the network. As a wireless channel experiences interference, multipath fading, hidden terminal problems, and stray packet drops might occur that should not be misclassified as selfishness.

Incentive-based approaches that include credit or reputation-based schemes proposed for MANETs are not suitable for static networks such as WMNs. In credit-based approaches [26], usually nodes earn credit by forwarding others' packets. However, a node in the periphery of the network is handicapped as it would not be able to earn credits by forwarding others' packets. In a MANET, as the topology changes are relatively frequent, any disadvantage due to improper location is usually mitigated. But in a WMN, the MRs are relatively static. In addition to this, the traffic in a WMN is primarily between the IGW and MRs, unlike in MANETs where it could be between any two MNs. And for the envisioned mesh applications like broadband Internet access, IGW is primarily the source of traffic flow as mesh clients download and upload data. Hence, credit-based schemes that restrict the traffic from an MP/MR by the amount of credits it possesses are not applicable in WMNs. A node could also build a false façade by initially forwarding packets dutifully and then dropping packets after becoming rich, which is counterintuitive to a credit-based detection scheme. In credit-based schemes, a node lacking sufficient credit would either buffer or blindly drop packets, making this approach highly unsuitable for real-time applications like VoIP and videoconferencing that need guaranteed QoS. Hence, we see that a credit-based scheme is nothing but a potpourri of loopholes for WMNs.

Next, we consider the compatibility of reputation schemes for WMNs. Although, they are not as problematic as credit-based approaches, they have some indigenous problems such as building mutual trust indices between neighboring nodes. Transformation of a monitored network activity into reputation is also a challenging task. In general, this knowledge is gained by eavesdropping on the neighboring node's transaction in promiscuous mode to check if it is forwarding packets [27]. The strength of this method lies in the assumption that an omnidirectional transmission as in 802.11 networks is used, which might not be feasible in multiradio and multichannel-capable WMNs. This also requires dedicated memory at each node. In a reputation scheme it is very important to discount old ratings and have a fading factor associated with all ratings, as a node with a good rating can become selfish at a later time. Hence, we need to focus on the problem of building a distributed monitoring system that weeds out in a timely manner the selfish MRs in the network.

In [28] we suggested the use of special localized detection agents called sink nodes for identifying selfish nodes in the network, and discuss

the appropriate action to be taken against such selfish nodes. The *sink nodes* are delegated the duty of policing their local neighborhood. All nodes in the network submit to their nearest sink node a summary of their transactions with their neighbors. These traffic reports consist of comprehensive information about the traffic exchanges of an MR with neighboring MRs. These reports are further analyzed individually by the sink nodes in a distributed fashion, occasionally consulting a central manager to break ties. The sink nodes then advertise the identity of the stealthy cheaters so that other MRs reroute their data along alternate paths and drop any traffic originating from selfish nodes. Thus, the packet delivery ratio of a good MR improves over time, and that of a selfish MR is kept in check. Bahl *et al.* [29] propose special agents called air monitors to manage enterprise wireless networks. They propose the use of desktops rather than relying solely on APs to monitor the wireless network. Thus, they create a low-cost management infrastructure with air monitors to monitor the wireless network. Such air monitors can be deployed at reliable nodes in a WMN to sense the traffic in their neighborhood and evaluate the integrity of the network.

There are several other issues that need to be addressed to ensure fairness in packet forwarding among nodes. A group of bad nodes might falsely implicate an innocent node by colluding. This stealthy slow poisoning by liars could inflict undue actions against well behaving nodes affecting their throughput. A good node entrapped by a misbehaving node is helpless in rerouting its traffic through alternate benign routes and totally under the mercy of its colluders. As a result, the performance of an entire network may be affected. There are several challenges to be met in this regard, which are summarized below.

#### *Open Research Issues*

- A reliable identity association is required so that a quarantined selfish node does not reappear with a new identity.
- An effective mechanism is needed to prevent source address spoofing, as a bad node could spoof the address of a good node and implicate it.
- A node on joining the network could act good in order to earn a good reputation for itself and could then commence its selfish activity under this facade.
- Even a quarantined selfish node should be given a chance to resocialize in the network after sometime. However, if resocializing is allowed, transient liars that alternate between good and bad behavior pose severe problem. Such vacillating nodes should be quarantined forever [26].

## Security Issues

The thrust of research in WMNs is primary focused on routing, and security is very much in its infancy. Just like any multihop wireless network, WMNs are also plagued with several security issues.

The openness of the WMN network makes it vulnerable to intruders, both external and internal. An external intruder can disrupt the routing by partitioning the network. An inside attacker in the form of compromised nodes is a much more pernicious attack as it could go undetected. An intruder can render the network dysfunctional in various ways such as route poisoning in the form of generating routing loops and misrouting of data, failing to forward traffic, executing a denial of service (DoS) attack, manipulating the content of payload, or a man-in-the-middle attack via masquerading. Hence, the fundamental security primitives of authentication, integrity, and confidentiality are very much essential for the correct functioning of WMNs. Authentication refers to the verification of identities of the communicating entities, integrity refers to the validity of the original message to guarantee that it has not been tampered with by an intermediate node, and confidentiality refers to the establishment of a secure channel to transmit cipher text that would be garblde to an intruder who is eavesdropping. Authentication, authorization, and accounting (AAA) services are generally provided in any wireless network by a centralized RADIUS server. The key challenge involved in implementing authentication using centralized servers like RADIUS lies in its scalability. As the RADIUS server is typically located at either the IGW or an MP in WMNs, when the number of mesh clients increases, the authentication overhead becomes excessively high. Hence, a scalable security solution has to be developed. Another main challenge is key management, which requires centralized issuing from an authority. But the absence of a central trusted authority and the hierarchical nature of MRs create additional overhead in key distribution. A scalable distributed scheme is required to distribute keys.

There are two dimensions to security in WMNs, which consist of MPs and mesh clients. As the interconnected MPs form the backbone of the network, the highest level of security is required here. Hence, all ongoing traffic should be encrypted using secure standards like 128- or 256-bit AES encryption, and all MPs should be authenticated in the network. An equal amount of attention should also be paid to mesh clients so as to prevent intruders in the network. This can be implemented by using authentication servers like RADIUS and 802.1x, and encrypting all the ongoing client traffic using standards like 802.11i/EAS/TKIP. There are various secure routing protocols in MANETs [30] that can be tailored to address route attacks in WMNs, but this requires careful consideration.

The 802.11 MAC protocol or another proprietary MAC protocol currently being used in WMNs is susceptible to several security flaws in the backoff procedure and Network Allocation Vector (NAV, used for carrier sensing). An attacker can insert large NAV values, thereby selfishly monopolizing the channel and resulting in a DoS attack on an innocent node, select a small backoff value to regain the channel, incorrectly place a de-authentication request to the AP for a neighboring node by spoofing their address, or congest the network by a DoS attack [31]. Hence, we also need a secure MAC proto-

An external intruder can disrupt the routing by partitioning the network. An inside attacker in the form of compromised nodes is a much more pernicious attack as it could go undetected.

There are two dimensions to security in WMNs which consists of MPs and mesh clients. As the interconnected MPs form the backbone of the network, the highest level of security is required here. Hence, all the ongoing traffic should be encrypted using secure standards.

col that would fix all these potential loopholes that could be exploited by an intruder.

As an additional check, continuous monitoring of the network by an intrusion detection system that helps detect misbehavior is required. Qui *et al.* [32] propose a novel troubleshooting technique to trace the exact root source of problems plaguing the multihop wireless network like packet dropping, link congestion, and MAC misbehavior. Physical and link layer parameters such as received signal strength, packet transmission, and retransmission counts are collected as trace data and reused to recreate the network scenario in a simulator like Qualnet for post-analysis. The simulator is then used as a fault diagnosis tool for identifying deviant behavior.

In order to maintain secure operation of WMNs, there are several open research avenues to be explored that are summarized below.

### *Open Research Issues*

- Authentication of MRs is an important issue to be addressed.
- Scalable key management technique needs to be developed.
- A secure multipath routing protocol is required.
- A multilayered security protocol that addresses all the above mentioned issues is desired to provide the highest level of protection.
- A distributed intrusion detection system is required for continuous monitoring of the network.

## Conclusion

WMNs introduce a new paradigm of true wireless Internet access, providing the maximum degree of flexibility at reduced cost to users. The scalability, self-configuring, and self-healing abilities of WMNs makes it a versatile technology expected to surpass other wireless technologies. As wireless mesh networks gain momentum in an endeavor to complement the wired backbone network, many issues are hindering its smooth progress. In this article we highlight some open research challenges at different layers, examine the feasibility of some state-of-the-art protocols, and discuss various issues.

Thus, the incumbent research proposals at each layer should strongly advocate a secure and scalable design seeking to further optimize the performance of WMNs. Although they have developed in leaps in recent years, there is still ample research work for radical progress of WMNs and true realization of Web-in-the-sky.

## References


[1] C. Cordeiro and D. P. Agrawal, *Ad Hoc & Sensor Networks, Theory and Applications*, World Scientific, Spring 2006.

[2] D. D. Couto *et al.*, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," *Proc. ACM MOBICOM*, 2003.

[3] R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks," *Proc. MOBICOM*, 2004.

[5] V. Jain *et al.*, "A Cross Layer MAC with Explicit Synchronization through Intelligent Feedback for Multiple Beam Antennas," *Proc. IEEE GLOBECOM*, 2005.

[6] S. Liese, D. Wu, and P. Mohapatra, "Experimental Characterization of an 802.11b Wireless Mesh Network," UC Davis Comp. Sci. Dept. tech. rep.

[7] V. Kawadia and P. R. Kumar, "A cautionary Perspective on Cross-Layer Design," *IEEE Wireless Commun.*, Feb. 2005.

[8] N. Nandiraju *et al.*, "A Novel Queue Management Mechanism for Improving Performance of Multihop Flows in IEEE 802.11s based Mesh Networks," *Proc. IPCCC*, 2006.

[9] R. Ramanathan, "Challenges: A Radically New Architecture for Next Generation Mobile Ad-Hoc Networks," *Proc. ACM MOBICOM*, 2005.

[10] J. So and N. Vaidya, "Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using A Single Transceiver," *Proc. MobiHOC 2004*.

[11] A. Adya *et al.*, "A Multi-Radio Unification Protocol for IEEE 802.11 Wireless Networks," *Proc. IEEE Conf. Broadband Networks*, 2004.

[12] P. Kyasanur and N. H. Vaidya, "Routing and Interface Assignment in Multi-Channel Multi-Interface Wireless Networks," *IEEE WCNC*, New Orleans, LA, Mar. 2005.

[13] K. Ramachandran *et al.*, "Interference-Aware Channel Assignment in Multi-Radio Wireless Mesh Networks," *IEEE INFOCOM*, 2006.

[14] A. Raniwala and T. Chiueh, "Architecture and Algorithms for an IEEE 802.11-Based Multi-Channel Wireless Mesh Network," *Proc. IEEE INFOCOM*, 2005.

[15] T. R. Jensen and B. Toft, *Graph Coloring Problems*, Wiley Interscience, 1995.

[16] M. Alicherry, R. Bhatia, and L. Li, "Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks," *Proc. MOBICOM*, 2005.

[17] J. Padhye *et al.*, "Estimation of Link Interference in Static Multi-hop Wireless Networks," *Proc. IMC 2005*.

[18] K. Ramachandran *et al.*, "On the Design and Implementation of Infrastructure Mesh Networks," *Proc. IEEE Wksp. Wireless Mesh Networks*, 2005.

[19] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *Proc. IEEE Trans. Info. Theory*, vol. 46, no. 2, 2000.

[20] M. Grossglauser and D. Tse, "Mobility Can Increase the Capacity of Ad Hoc Wireless Networks," *Proc. IEEE INFOCOM,* 2001.

[21] M. Gastpar and M. Vetterli, "On the Capacity of Wireless Networks: The Relay Case," *Proc. IEEE INFOCOM*, 2004.

[22] A. E. Gamal *et al.*, "Throughput-Delay Trade-off in Wireless Networks," *Proc. IEEE INFOCOM*, 2004.

[23] J. Jun and M. L. Sichitiu, "The Nominal Capacity of Wireless Mesh Networks," *IEEE Wireless Commun.*, 2003.

[24] K. Jain *et al.*, "Impact of Interference on Multihop Wireless Network Performance," *Proc. ACM MOBICOM*, 2003.

[24] I. F. Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks," *Proc. IEEE Radio Commun.*, Sept. 2005.

[25] P. Kyasanur and N. Vaidya, "Capacity of Multi-Channel Wireless Networks: Impact of Number of Channels and Interfaces," *Proc. MOBICOM*, 2005.

[26] Y. Yoo, S. Ahn, and D. P. Agrawal, "A Credit-Payment Scheme for Packet Forwarding Fairness in Mobile Ad Hoc Networks," *Proc. IEEE ICC*, 2005.

[27] S. Marti *et al.*, "Mitigating Router Misbehavior in Mobile Ad-Hoc Networks," *Proc. MOBICOM*, 2000.

[28] L. Santhanam *et al.*, "Distributed Self-policing Architecture for Packet Forwarding Fairness in Wireless Mesh Networks," to Appear in *11th IFIP Int'l. Conf. Pers. Wireless Commun.*, Albacete, Spain, Sept. 20–22, 2006.

[29] P. Bahl *et al.*, "DAIR: A Framework for Troubleshooting Enterprise Wireless Networks Using Desktop Infrastructure," *Proc. ACM HotNets-IV 2005*, College Park, MD, 2005.

[30] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure on Demand Routing Protocol for Ad Hoc Networks," *Proc. ACM MOBICOM*, 2002, pp. 12–23.

[31] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *Proc. IEEE MILCOM*, 2002.

[32] L. Qui *et al.*, "Troubleshooting Multihop Wireless Networks," *Proc. SIGMETRICS* (extended abstract), June 2005.


## Additional Reading


[1] S. Zhong, Y. Yang, and J. Chen, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad Hoc Networks," *Proc. IEEE INFOCOM*, 2003.


## Biographies


DHARMA P. AGRAWAL [M'74, F'87] (dpa@ececs.uc.edu) is the Ohio Board of Regents Distinguished Professor of Computer Science and Engineering and founding director of the Center for Distributed and Mobile Computing in the

Department of Electrical and Communications Engineering and Computer Science (ECECS), University of Cincinnati, Onio. He has been a faculty member at North Carolina State University, Raleigh, (1982–1998) and Wayne State University, Detroit, Michigan (1977–1982). His current research interests are energy-efficient routing and information retrieval in sensor and mesh networks, QoS in integrated wireless networks, use of smart multibeam directional antennas for enhanced QoS, and various aspects of sensor networks including environmental monitoring and secured communication in ad hoc and sensor networks. His co-authored textbook, *Introduction to Wireless and Mobile Systems* (Thomson) has been adopted throughout the world and revolutionized the way the course is taught. His second co-authored textbook, *Ad Hoc and Sensor Networks*, has just been published. He has served as an editor of *IEEE Computer* magazine, *IEEE Transactions on Computers*, and the *International Journal of High Speed Computing*. He is an editor for the *Journal of Parallel and Distributed Systems*, *International Journal on Distributed Sensor Networks*, *International Journal of Ad Hoc and Ubiquitous Computing*, *International Journal of Ad Hoc & Sensor Wireless Networks*, and *Journal of Information Assurance and Security*. He has been Program Chair and General Chair for numerous international conferences and meetings. He has received numerous certificates and awards from the IEEE Computer Society. He was awarded a Third Millennium Medal by the IEEE for his outstanding contributions. He has also delivered keynote speeches at five international conferences. He also has four patents and 16 patent disclosures in wireless networking. He has been selected as a Fulbright Senior Specialist for a duration of five years. He is a Fellow of the ACM, AAAS, and WIF.

NAGESH NANDIRAJU [S] (nandirns@ececs.uc.edu) is currently pursuing his doctoral studies in the Department of ECECS, University of Cincinnati. He is working as a research assistant in the Center for Distributed and Mobile Computing at the University of Cincinnati. He received his B.E in computer science and engineering first class with distinction from the University of Pune in 2001. His research interests are in the broad area of wireless ad hoc and infrastructured networks. His work includes performance evaluation and design of efficient MAC and routing protocols for multihop wireless ad hoc, mesh, and sensor networks. He has prior work experience at the National Institute of Technology, Silchar, India.

DEEPTI NANDIRAJU (nandirds@ececs.uc.edu) has been a doctoral student in the Center for Distributed and Mobile Computing at the University of Cincinnati since 2004. She received her B.S. degree in 2001 and M.S. degree in 2003 with a gold medal in computer science from Assam University, Silchar, India. Her current research interests are in the area of fairness issues and routing protocols for wireless ad hoc and mesh networks.

LAKSHMI SANTHANAM (santhal@ececs.uc.edu) received her B.E. degree in computer science and engineering from the University of Madras, India, in 2003. She is currently a doctoral student working as a research assistant in the Center for Distributed and Mobile Computing at the University of Cincinnati. Her research interests include detection of selfish behavior, traceback of DoS attacks, combating DoS attacks, intrusion detection in multihop networks, and other security concerns in wireless ad hoc and mesh networks.

BING HE [S '01](heb@ececs.uc.edu) is a Ph.D. student in computer engineering at the Center for Distributed and Mobile Computing in the Department of ECECS, University of Cincinnati. His current research interests include architecture and capacity of wireless mesh networks, and resource allocation in 802.16 wireless MANs. He received his B.S. degree in communication engineering and M.S. degree in signal and information processing from Northern Jiaotong University of China. He has been an engineer at Honeywell Technology Solutions Laboratory in China.

JUNFANG WANG (wangjf@ececs.uc.edu) received her B.S. degree in computer science from Northeastern University (, China, and her M.S. degree in computer science from Nanjing University of Aeronautics & Astronautics, China. She was previously a senior software engineer and team manager at Zhongxing Telecom Company, China, working on the PCS and has a patent pending on it. Currently she is pursuing her Ph.D. degree in the Center for Distributed and Mobile Computing in the Department of ECECS, University of Cincinnati. Her current research interests include positioning techniques, channel assignment, and cross-layer routing in wireless mesh networks, and interference control in WLAN and wireless mesh networks.

Thus, the incumbent research proposals at each layer should strongly advocate a secure and scalable design seeking to further optimize the performance of WMNs. There is still ample research work for radical progress of WMNs and a true realization of Web-in-the-sky.