Autonomic Fault Management for Wireless Mesh Networks

Nan Li,[†] Guanling Chen,[†] and Meiyuan Zhao[‡]
[†]Department of Computer Science, University of Massachusetts at Lowell
[†]{nli, glchen}@cs.uml.edu
[‡]Intel Technology and Research
[‡]meiyuan.zhao@intel.com

Abstract

Wireless Mesh Network (WMN) provides a cheaper option for backhauls that can be leveraged to provide low-cost access services. Compared to conventional wireless LANs, the benefits of a WMN include greater range because of packet relaying and higher throughput because of shorter hops. A WMN, however, may be subject to a variety of faults that are hard to diagnose manually. In this paper we discuss Autonomic Fault Management (AFM) to automate many of the fault management tasks by continuously monitoring network condition for self-awareness, analyzing the fault when it is detected for self-diagnosis, and taking adaptation actions for self-recovery. Thus AFM can reduce potential human errors and can respond to faults faster, effectively reducing the network downtime. We review challenges and possible solutions for three important components of an AFM: network measurements, fault diagnosis, and fault recovery. We also briefly discuss the security issue for AFM.

1 Introduction

Compared to the traditional wired network, Wireless Mesh Network (WMN) provides a low-cost access services with much chapter deployment cost. Compared to conventional wireless LANs, the benefits of a WMN include greater range because of packet relaying, and higher throughput because of shorter hops. Typical WMN applications include intelligent transportation, public safety, sensing backbone, and community access [3]. To May of last year, there are more than 400 U.S. cities, towns and counties that were deploying or planning to deploy wireless networks. In industry, there are several big vendors, including Motorola, Nortel Networks, Tropos Networks, and Cisco Systems, providing the mesh network equipment. Table 1 lists some big cities' municipal wireless projects [1].

A WMN consists of one (or more) Internet gateway nodes and a set of mesh nodes forming a multi-hop network. A mesh node may contain one or more radios and provide network access services to the clients. A WMN could be set up by a single entity (such as an ISP) or by multiple parties (such as voluntary users). IEEE 802.11s Task Group is extending the IEEE 802.11 architecture and protocol for providing the functionality of an extended service set mesh, while several companies have been selling their proprietary solutions for both indoor and outdoor mesh products. According to Infonetics Research, outdoor mesh equipment sales jumped 38% to $121.40 million in the 3rd quarter of 2006 and they are forecast to reach $1.17 billion in 2009 [14].

A WMN, however, may be subject to a variety of faults (see Section 2), which can manifest themselves as abnormally low throughput, excessive delay and jitter, non-responding nodes, intermittent or no connectivities, and so on. There are a large number of potential factors, benign or malicious, may cause a fault. The quality of wireless links is influenced by the physical environment, such as obstacles, weather, and noise. Nearby mesh nodes and stations may content for the shared wireless medium, which may lead to problems including hidden terminal and capture effect, and is subject to bandwidth cheating [6]. The multi-hop nature of WMNs requires cooperative packet relay among mesh nodes, where a malicious participant may attack the routing and forwarding functions to bring the network into a dismal state. Device or protocol misconfiguration may also cause a fault. For example, some mesh protocols

Location	Size of Project	Business Model	Status	Vendors
Boston	Not specified	Publicly funded by nonprofit arm	Cover entire city by end of 2008	various vendors
Houston	600 square miles	Earthlink builds for free and chages subs	Announced in Feb 2007: set for completion in 2009	EarthLink
Philadelphia	135 square miles	Public/private partnership	Fall 2007	EarthLink, Wireless Philadelphia
San Francisco	50 square miles	Privately funded, ad-supported and/or fee-based	Agreement awaiting city board of supervisors approval	EarthLink, Google, Tropos

Table 1: Some Municipal Wireless Projects

require each node be configured in the same subnet. Non-compliant nodes may not join the mesh even if they have link-layer connectivity.

Typical fault management tasks include detecting and identifying faults, isolating faults and determining the root cause, and recovering from the faults. A manual approach requires accepting and acting on error detection notifications, maintaining and examining error logs, tracing and identifying faults by examining environmental changes and database information, carrying out sequences of diagnostics tests, and correcting faults by reconfiguring/restarting/replacing network elements. Manual fault management is usually a time-consuming and tedious task, requiring a human expert to have a thorough knowledge of the network and to comprehend a large amount of information.

It is desirable to provide Autonomic Fault Management (AFM) for any large-scale network supporting many users and a diverse set of applications. AFM aims to automate many of the fault management tasks by continuously monitoring network condition for self-awareness, analyzing the fault after it is detected for self-diagnosis, and taking adaptation actions for self-recovery. Thus AFM can reduce potential human errors and can respond to faults faster, thus effectively reducing the network downtime.

AFM is a critical component for network self-management and it is particularly suitable for WMNs, where faults may occur more frequently than conventional networks because of unreliable wireless links and harsh outdoor environment. Instead of having fairly concentrated network elements with local administrators, a WMN may have mesh nodes distributed over a large geographical space where the nodes could be located on top of roofs and light-poles, making them far-less accessible for in-field testing. Remote manual diagnosis needs interactive testing but may not be effective for WMNs due to dynamic multi-hop routing, unreliable wireless links, limited bandwidth, and relatively long delay [12], particularly when a fault has occurred. Further more, some WMNs do not have a single management entity, such as the community mesh network. It is infeasible to ask individual users to management these self-forming networks and AFM is required.

AFM is a fairly young research field, in this paper we discuss how AFM can be used for WMNs. We review challenges and possible solutions for three important components of an AFM: network measurements, fault diagnosis, and fault recovery. We also briefly discuss the security issue for AFM.

In the rest of this paper, we present the fault category of WMN in Section 2, which is the background of discussion AFM system. The network measurements is described in section 3. The fault diagnosis and fault recovery are described in section 4 and 5 respectively. We discuss the security issues of WMN in section 6. The conclusion is in section 7.

2 Background

There are a variety of complex faults that may occur in a WMN, which can be roughly divided into four categories. Our further discussions of AFM are based on those faults.

- Transmission link fault. A wireless link may experience excessive loss rate or prolonged delays. Possible reasons may include external noises, multi-path fading, strong interferences, hidden terminal and capture effects, and misbehaving clients [21].
- Network element fault. Individual mesh devices may fail in several ways, including hardware failure, power supply fails, and software crashes. For example, it has been demonstrated that several wireless drivers may be exploited to crash and even take over the vulnerable devices by an attacker.
- Mesh protocol fault. While many mesh routing protocols are designed to automatically recover from path failures, they may still introduce some undesired problems. For example, under certain conditions, some routing protocols will create a routing loop or a black hole. Overly agile routing protocols may cause route flapping and degrade network throughput [18]. An adversary may also intentionally disrupt routing and forwarding functions in a WMN [9].
- Traffic congestion. As the offered load approaches or exceeds the link or network capacity, a WMN may experience significant congestion or even collapse if not handled appropriately. The nodes near the gateway may experience more congestion due to aggregated packet relay [4].

3 Network Measurements

A key component for AFM is the network measurement, which serves two purposes. One is for AFM to detect the presence of a fault (**fault detection**), and the other is for AFM to identify the type of the fault, localize the fault, and pinpoint the root cause of the fault (**fault diagnosis**). Typically fault diagnosis is more heavy weight and requires more information, thus it is desirable to save network overhead by running a light-weight measurement process for fault detection prior to further diagnosis. The measurements could be either passive or active, which incurs additional network overhead [22]. Thus it is desirable to use passive measurements for fault detection and active measurements for further fault diagnosis (Section 4).

Which network measurements are useful depends on the types of faults to be managed. There are roughly three categories of network measurements: node-level, neighborhood, and global measurements.

Node-level measurements. A mesh node may monitor itself on resource usage, such as CPU and memory usage, to estimate its own health status and predict possible faults. It may also measure channel conditions such as the external noise level, signal strength of its neighbors, and its perceived medium utilization. This information is location-specific and usually hard to be measured by other nodes. A mesh node may also collect statistics on link quality, relayed and dropped packets, queue length, and so on. Other configuration parameters, such as transmission power level, routing table, neighbor list, firewall rules, may also be collected for fault diagnosis.

Neighborhood measurements. A mesh node may cooperatively work with its neighbors to provide some measurements, such as accurate link quality [10]. For example, a routing protocol may use link quality as the basis of path-selection metrics, such as Expected Transmission Count (ETX) [5] and Weighted Cumulative Expected Transmission Time (WCETT) [8]. Because of the shared wireless medium, a mesh node may also overhear its neighbor's transmission and thus can collect relevant statistics for fault diagnosis. For example, a mesh node may use the difference of a neighbor's received and relayed packets as an indication of misbehaving forwarding function [24].

Network-wide measurements. It may also be necessary to collect network-wide measurements, such as network topology and routing state, to detect routing anomalies including loops and flapping. Channel conditions over the network as a whole should be considered when setting radio channel to achieve both well connected topology and high network throughput [19].

A single node's observations are usually incomplete and it is necessary to correlate measurements from multiple sources for fault diagnosis. A centralized AFM collects all network measurement data

and performs fault detection and diagnosis. The advantage is having a more complete network observations and a natural vintage point for logging. The disadvantage is that to obtain further measurement is hard during fault has caused route disruption and even network partition. For example, the AFM may need a long time or may not even be able to access the node-level measurement stored in Management Information Base (MIB) during faults. One possible solution is to leverage some predictive methods, so the measurement information will be disseminated when a fault is imminent. Another solution is to periodically disseminate measurement data, such as using a gossip protocol, so the centralized AFM will at least have partial information when the fault occurs. If a mesh network has multiple gateways, the measurement data may be disseminated through other gateways if the path to original preferred gateway is disrupted [17].

A distributed approach of AFM does not require hauling all measurement data to a centralized location, saving bandwidth and avoiding the single point of failure [2]. For example, a local fault may be easily detected and diagnosed by cooperating among adjacent nodes. On the other hand, fault diagnosis may take valuable resources if performed by the nodes themselves, which may degrade routing performance. One possibility is for the mesh nodes self-organized into several clusters, each one forming a management domain. A cluster head is responsible for local fault management and the cluster heads may communicate among themselves for detecting and diagnosing network-wide anomalies.

4 Fault Diagnosis Algorithms

Fault diagnosis typically includes fault isolation (where is the fault located), fault identification (what is the type of the detected fault), and root cause analysis (what has caused the fault). With sufficient measurement, it is relatively easy to locate the fault and determine whether the fault is a link or node failure, protocol error, or traffic congestion. It is, however, challenging to pinpoint the root cause of the fault, based on which the AFM makes autonomic recovery decisions to correct the fault.

Some of existing solutions make implicit assumptions about the root cause and may make inappropriate adaptations. For example, it is well known that TCP assumes packet loss is always caused by congestion and then slows down the sender for congestion avoidance, which leads to bad performance over error-prone wireless links. For the frame loss at the MAC layer, 802.11 makes conflicting assumptions: it backs off sender assuming the frame loss is caused by contention, and it may also lower the transmission rate assuming the frame loss is caused by bad channel condition. The link throughput can be significantly improved if rate adaptation considers the root cause of the bad link quality [23].

Some of existing solutions try to recover from the fault without determining the root cause. For example, several routing protocols try to repair the paths once a link failure is detected by selecting other links. This oblivious fault recovery, however, could be expensive and there may be opportunities to quickly recover the fault with less cost by reacting to the root cause. For example, a mesh node may simply increase its transmission power level if a link degrades because of obstacles, or it can switch channel (with its neighbors) if the current channel has strong noise or is too busy.

Fault diagnosis essentially determines the root causes from observed symptoms, such as abnormal events derived from the network measurements. One popular approach is to use an expert system, which contains diagnostic rules mimicking how a human expert might perform systematic fault analysis. These rules are typically derived through knowledge engineering by extracting heuristics from human experts. This approach has been demonstrated useful in medical applications such as disease diagnosis. It is, however, limited for fault diagnosis in communication networks due to the large number of fault types, the complexity of network element interactions, and the overwhelming amount of measurement information. Even a human expert may have difficulties understanding the fault, rendering knowledge engineering for an expert system an expensive approach.

Another approach is to derive these diagnostic rules using machine learning. Given a set of symptoms and a set of potential faults, it is possible to build a cause-effect (or dependency) model using a variety of techniques, such as neural network, decision trees, data mining, and many others. These models then classify observed symptoms into underlying faults. For example, Zhang and Lee use a classification algorithm, RIPPER, to identify malicious routing table updates [25]. These learning-based approaches consist of supervised algorithms that require offline training data containing normal traffic and faults.

Usually it is difficult to obtain such data with all fault scenarios and traffic conditions. These algorithms must also be robust to natural variations in a wireless environment, often giving probabilistic results at best.

Previously discussed approaches may be effective for diagnosing common faults with well-crafted rules, but it is cumbersome to handle new fault types or new mesh protocols. It is necessary to obtain new training data and update many rules. Thus is desirable to have a general diagnostic engine that can be easily updated and extended.

One may borrow model-based diagnosis approach, originally designed to diagnose component failures within a circuit [7]. The key idea is to build a structural and behavioral model, where the structure is a acyclic graph representing influence relationship among components and the behaviors are expected performance output. The combination of structure and expected behaviors can by used to systematically track down and return the root cause (faulty component). In the context of diagnosing communication networks, the diagnosis structure must be constructed by network measurements because the topology is not known beforehand, and the behaviors are expected performance. Once the network model is obtained, it is possible to detect a fault if the observed performance does not match what is predicted by the model. Then a diagnosis engine can iteratively inject a fault into the network model and if the prediction of the updated model matches with the measured performance, the injected fault is then considered as the root cause. Qiu et al. has used network measurement to build simulation models for diagnosing packet dropping, link congestion, external noise sources, and MAC misbehavior in a WMN [16].

Model-based diagnosis is flexible in the sense that it can be easily extended to handle new fault types, while the network model is constructed automatically and the reasoning logic remains more or less the same. The challenge here is to build accurate network models, including physical channels, network topology, and traffic workload, by network measurements, so the prediction can be useful for diagnosis. Like all other diagnosis approaches, it is challenging if there are multiple faults occurred in the network.

5 Autonomic Fault Recovery

Once a fault is detected and diagnosed, AFM performs automated actions to repair the fault, bringing the WMN to a desirable state. In some cases, the fault can be repaired in a localized fashion without global impact. For example, a transmitter may adjust its transmission rate to accommodate bad channel condition or back off in face of excessive contention. If a mesh node is not forwarding all the packets as expected, its neighboring nodes may blacklist it from routing if that node is determined to be selfish, or reallocate traffic if that node is simply congested. In these scenarios, better recovery methods can be achieved if the root causes of the fault is known. For example, a robust mechanism to deal with packet loss at MAC layer is to dynamically change transmission rate or adaptively turn on RTS based on sender's estimation whether the loss is caused by bad channel condition or by hidden terminal (contention) [23].

Some of the adaptations, however, may have a rippling effect over the whole network. For example, when a link is heavily congested or degraded by excessive noise, a simple recovery action is to have the two mesh nodes of that link switch to another channel with less spectrum activity. However this may require a large portion or all of the mesh nodes to switch channels, particularly for a single-radio WMN, so the network topology stays connected. In this case, the conditions of all channels at affected mesh nodes should be considered as a whole when deciding which channel to switch to.

If the link degradation or disruption does not partition the network, some mesh routing protocols are capable of repairing affected paths by automatically choosing other links to minimize some cost metrics, such as ETX [5]. Overly agile protocol reactions, however, may lead to route flapping [18]. This autonomic behavior may increase the network overhead by flooding the route repair control messages without much gain of throughput. One possible way to counter this effect is to use flap damping, but it may cause persistent oscillation in the network due to the adverse interactions between flap damping and route convergence like BGP [13]. Thus autonomic fault recovery must be aware of interacting control loops that may result in complex and hard-to-understand behaviors [15].

It is desirable to have a holistic approach for fault recovery in WMN, particularly when there are more than one possible recovery choices. As the link disruption example, it is sometimes not obvious which adaptation works better in current network situation. The challenge is that different adaptations

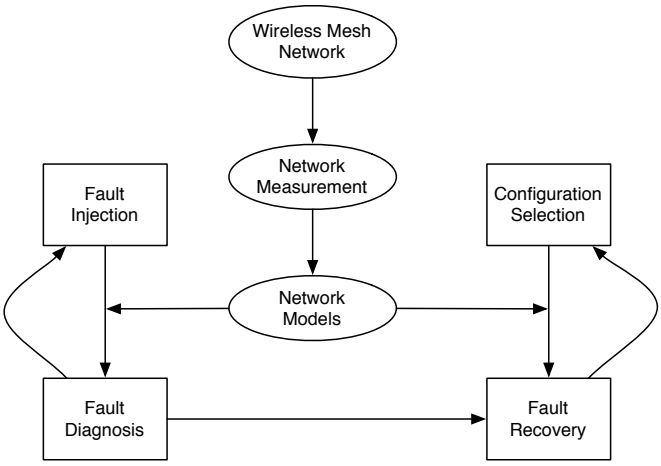

Figure 1: Model-based fault management.

have different trade-offs. For example, increasing transmission power level may improve the link quality and the topology robustness (increased number of neighbors), but it also increases self-interference and may reduce overall throughput. Switching channels at one location to avoid external noises may require channel reassignments at another location, to have a connected topology, where the channel condition could be bad. It is thus inherently challenging to balance various tradeoff for WMNs in a real-world environment.

A centralized approach is to build analytical or simulation models using network measurements, to match the WMN being controlled. When a fault occurs, the centralized manager can feed various configurations into the network models. A configuration for a mesh node may include the gateway selection, channel assignment, transmission power selection, routing table entries, and so on. The next step is to compare various configurations quantitatively using desired metrics, such as average throughput or packet delay. The optimal configuration is then translated to recovery actions taken by the mesh nodes. The configuration space, however, could be huge depending on the number of configuration parameters and the mesh nodes. One can use heuristics to aggressively prune the search space for better performance. For example, Raniwala et al. use network traffic as measurement input and jointly assign channels and routing tables in a multi-radio WMN by iterating the channel/route configurations to achieve improved cross-section goodput [20]. Figure 1 shows the measurement-derived models can be used by both iterative fault diagnosis (Section 4) and fault recovery.

A centralized manager is suitable for a small-scale WMN, where link failures are infrequent (unlike mobile ad hoc networks where mobility often breaks links) and network partitions are rare (with appropriate planning and multiple gateways). It is, however, not always suitable to have a centralized entity for a WMN, particularly for community networks where mesh nodes are set up by voluntary users. Thus a distributed solution is desired for these self-forming WMNs. One approach is to consider each mesh node as an agent, and all agents negotiate among themselves for a configuration that achieves optimal overall network performance. When a fault is detected an diagnosed, a subset or all of the agents re-negotiate appropriate configurations. This approach can be formulated as Distributed Constraint Optimization Problem (DCOP). The constraints could be specified for multiple objectives, such as each node should have at least three neighbors (for robustness), or each neighbor should have at least two disjoint paths to some gateways, the average throughput should be maximized, and so on. The DCOP approach has been applied in sensor networks, to balance the network lifetime, detection accuracy, and sensor coverage [11].

These autonomic fault recovery approaches need to address three significant challenges. First the network measurements must allow accurate reconstructions of network models, otherwise the computed recovery actions could be misleading. Another challenge is that finding a suitable configuration in a large solution space must be fast enough, otherwise the network dynamics may render the returned

solution no longer applicable. Finally, an AFM must support human understanding by providing logs and explanation on its reasoning logic of fault diagnosis and recovery process. This will increase the user confidence for better adoption. Mortier and K?c?man also suggest that an AFM should be self-monitoring and self-validating to avoid costly mistakes [15].

6 Security Issues

Network measurements are used for fault diagnosis and eventually network adaptation for fault recovery. An attacker may intentionally report false network measurements to confuse and mislead the AFM. It is thus important to authorize the measurement sources, guarantee the measurement data integrity, and authenticate the measurement sources and data. Typically cryptographic protocols can be used to provide these security properties. In some cases, such as the community mesh network, it may not be feasible to ask each user to obtain certificates used to authenticate the mesh nodes. The question then becomes how to perform meaningful fault diagnosis and recovery in this kind of environment without assuming cooperation. One possibility is to introduce reputation to represent the level of trust or game theory, but this line of research is still in an early stage.

An adversary may also influence the AFM without compromising the security. For example, a selfish user or a competitor can generate excessive noise to divert a WMN to other channels so his own wireless network can occupy a particular channel for better performance. An attacker may periodically disrupt selected links to cause excessive routing repairs or frequent route flapping, rendering targeted WMN less effective. If the attacker causes enough number of fault alerts and put AFM under heavy load diagnosing these faults, he can carry out the real attack that may go unnoticed. These are hard problems for an AFM and deserve attentions from the research community.

7 Summary

In summary, Autonomic Fault Management (AFM) is a critical component for self-managing WMNs. AFM is a young and exciting field that requires significant algorithm and system research in network measurement, fault diagnosis, and fault recovery. Instead of providing point solutions, it is particularly desirable but challenging to provide a general and secure AFM framework to address a variety of complex faults.

References

[1] White paper, state of the municipal wifi market, 2007.

[2] Remi Badonnel, Radu State, and Olivier Festor. Self-configurable fault monitoring in ad-hoc networks. *Ad Hoc Netw.*, 6(3):458–473, 2008.

[3] Raffaele Bruno, Marco Conti, and Enrico Gregori. Mesh Networks: Commodity Multihop Ad Hoc Networks. *IEEE Communications*, 43(3):123–131, March 2005.

[4] K.R. Chowdhury and I.F. Akyildiz. Cognitive wireless mesh networks with dynamic spectrum access. *Selected Areas in Communications, IEEE Journal on*, 26(1):168–181, Jan. 2008.

[5] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking*, pages 134–146, San Diego, CA, September 2003.

[6] Saumitra M. Das, Dimitrios Koutsonikolas, and Y. Charlie Hu. Measurement-based characterization of a wireless mesh network. In *Handbook of Wireless Mesh and Sensor Networking*. McGraw-Hill International, 2008.

[7] Johan de Kleer and Brian C. Williams. Diagnosis with behavioral modes. In Walter Hamscher, Johan de Kleer, and Luca Console, editors, *Readings in model-based diagnosis*, pages 124–130. Morgan Kaufmann Publishers, 1992.

[8] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *Proceedings of the Tenth Annual International Conference on Mobile Computing and Networking*, pages 114–128, Philadelphia, PA, September 2004.

[9] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Networks*, 1(2–3), September 2003.

[10] Kyu-Han Kim and Kang G. Shin. On accurate measurement of link quality in multi-hop wireless mesh networks. In *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking*, pages 38–49, Los Angeles, CA, September 2006.

[11] Victor Lesser, Charles L. Ortiz, and Milind Tambe. *Distributed Sensor Networks: A Multiagent Perspective*. Springer, September 2006.

[12] Nan Li, Bo Yan, and Guanling Chen. A measurement study on wireless camera networks. In *Proceedings of the Second International Conference on Distributed Smart Camera (ICDSC)*, Stanford, CA, September 2008.

[13] Zhuoqing Morley Mao, Ramesh Govindan, George Varghese, and Randy H. Katz. Route flap damping exacerbates internet routing convergence. In *Proceedings of the 2002 ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pages 221–233, Pittsburgh, PA, August 2002.

[14] Wi-Fi, WiMAX, Wireless Mesh Network Equipment Sales All Increase in 3Q06. Infonetics Research Market Share and Forcasts.

[15] Richard Mortier and Emre Kcman. Autonomic Network Management: Some Pragmatic Considerations. In *Proceedings of the ACM SIGCOMM Workshop on Internet Network Management*, Pisa, Italy, September 2006.

[16] Lili Qiu, Paramvir Bahl, Ananth Rao, and Lidong Zhou. Troubleshooting Wireless Mesh Networks. *ACM SIGCOMM Computer Communication Review*, 36(5):17–28, October 2006.

[17] K.N. Ramachandran, E.M. Belding-Royer, and K.C. Almeroth. DAMON: a distributed architecture for monitoring multi-hop mobile networks. In *Proceedings of the 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks*, pages 601–609, Santa Clara, CA, October 2004.

[18] Krishna Ramachandran, Irfan Sheriff, Elizabeth Belding, and Kevin Almeroth. Routing stability in static wireless mesh networks. In *Proceedings of Passive and Active Measurement Workshop (PAM)*, Louvain-la-neuve, Belgium, April 2007.

[19] A. Raniwala and Chiueh Tzi-cker. Architecture and algorithms for an IEEE 802.1 1 -based multi-channel wireless mesh network. In *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pages 2223–2234, Miami, FL, March 2005.

[20] Ashish Raniwala, Kartik Gopalan, and Tzi cker Chiueh. Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks. *ACM SIGMOBILE Mobile Computing and Communication Review*, 8(2), April 2004.

[21] Maxim Raya, Jean-Pierre Hubaux, and Imad Aad. DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots. In *Proceedings of the Second International Conference on Mobile Systems, Applications, and Services*, pages 84–97, Boston, MA, June 2004.

[22] Sonesh Surana, Rabin Patra, Sergiu Nedevschi, Manuel Ramos, Lakshminarayanan Subramanian, Yahel Ben-David, and Eric Brewer. Beyond pilots: keeping rural wireless networks alive. In *NSDI'08: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation*, pages 119–132, Berkeley, CA, USA, 2008. USENIX Association.

[23] Starsky H. Y. Wong, Songwu Lu, Hao Yang, and Vaduvur Bharghavan. Robust rate adaptation for 802.11 wireless networks. In *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking*, pages 146–157, Los Angeles, CA, September 2006.

[24] Hao Yang, James Shu, Xiaoqiao Meng, and Songwu Lu. SCAN: Self-organized Network Layer Security in Mobile Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 24:261–273, February 2006.

[25] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking*, pages 275–283, Boston, MA, August 2000.