Beyond Pilots: Keeping Rural Wireless Networks Alive

Sonesh Surana* Rabin Patra* Sergiu Nedevschi* Manuel Ramos†
Lakshminarayanan Subramanian‡ Yahel Ben-David§ Eric Brewer* ¶

Very few computer systems that have ever been deployed in rural areas in developing regions have been operational and sustainable in the long term — most such systems have not gone beyond the pilot phase. This paper describes our experiences in deploying and maintaining two rural WiFi-based long-distance networks over the last three years: (a) the Aravind network interconnecting rural eye hospitals in South India which served so far over 30,000 patients, and currently serves about 2500 patients per month, and (b) the AirJaldi network in North India that provides Internet access and VoIP services to over 10,000 users in rural mountainous terrain.

In this paper, we elaborate upon the various systems challenges we had to overcome to make both these networks operationally sustainable. We explore system design issues around simplifying system management issues such as monitoring and administration, and also around improving sustainability in the context of rural challenges such as low-quality power, limited local expertise, lack of remote management opportunities (bad connectivity), and limited budgets. Based on initial successes, the pilot network at Aravind is now scaling from 5 centers to 50, with a target of 500,000 patients per year and the AirJaldi model is being now replicated in Rajasthan and Dehradun.

1 Introduction

The penetration of computer systems in the rural developing world has been abysmally low. Several efforts around the world [2, 13, 15] that have tried to deploy low-cost computers, kiosks and other types of systems have struggled to remain viable, and almost none are able to remain operational over the long haul. The reasons for these failures vary, but at the core is an under appreciation of all the obstacles that limit the transition from a successful pilot, of which there are many, to a truly sustainable system. In addition to financial obstacles, these include problems with power and equipment, environmental issues, and an ongoing need for trained local staff (as trained staff move on to better jobs).

For example, one excellent pilot project in Tanzania used a PC to collate data on the actual causes of child deaths and was able to reduce child mortality in two districts from 16% to 9% [28]. Despite this clear success, national deployment never occurred largely due to lack of ongoing funding, shortage of trained staff for a larger deployment, and the complexity of IT solutions.

This under appreciation also stems from the tendency of researchers (ourselves included) to focus on the sexy parts of a deployment, such as higher performance or a highly visible pilot. Real impact requires a sustained presence, and thus the operational challenges must be viewed as a first-class research topic. Analogous to research on high availability, we find that we must document and categorize the actual causes of operational problems and take a broad systemic view to address the problems well. Even though solving specific incidents tends to be straightforward, addressing the wide range of ongoing issues is much harder.

This paper addresses operational sustainability for rural WiFi-based connectivity solutions. We describe our experiences in deploying and maintaining two rural wireless systems based on point-to-point WiFi links. Our prior work on *WiFi-based Long Distance Networks (WiLDNet)* [23] developed a low-cost high-bandwidth long-distance solution, and it has since been deployed successfully in several developing regions. We present real-world validation of the links, but the primary contribution is the exploration of the operational challenges of two rural networks: the Aravind telemedicine network in southern India and the AirJaldi community network in northern India.

The Aravind network uses WiLDNet to interconnect rural vision centers with their main hospitals. Currently this network serves 9 vision centers and has so far catered to roughly 30,000 patients at a rate of 2500 patients every month. Over 3000 patients have received significant vision improvement using this network. The AirJaldi network currently provides Internet access and VoIP services to over 10,000 users in a rural mountainous terrain. We present a broad range of operational issues from two years of deployment experience with these networks, including both detailed specifics about operational is-

*University of California, Berkeley
†University of the Philippines
‡New York University
§AirJaldi, Dharamsala, India
¶Intel Research, Berkeley

sues and our experience with corresponding evolutionary changes. We also draw broad lessons from the deployments that apply more broadly.

In Section 2 we validate the sufficiency of real-world WiLD performance, and outline the challenges to operational sustainability. Section 3 provides some background for both the Aravind and AirJaldi projects. In Section 4, we document many of our experiences with system failures, and then in Section 5 present design changes at various layers to respond to these issues. Sections 6 and 7 present related work and our conclusions.

2 Motivation

In this section, we confirm good performance of WiLDNet links in real-world deployments, and then outline the operational challenges, which form the primary remaining obstacle to sustained impact.

2.1 Real-World Link Performance

Existing work [6, 23, 25, 30, 31] on rural networking has focused on making WiFi-based long-distance point-to-point links feasible. The primary goal has been to achieve high performance, typically expressed as high throughput and low packet loss.

In prior work, we have addressed channel-induced and protocol-induced losses in long-distance settings [30] by creating WiLDNet: a TDMA-based MAC with adaptive loss-recovery mechanisms [23]. We have shown a 2–5 fold increase in TCP/UDP throughput (along with significantly reduced loss rates) in comparison to the best throughput achievable by the standard 802.11 MAC. We showed these improvements on real medium-distance links and emulated long-distance links.

We confirm the emulated results with data from several real long-distance links in developing regions. Working with Ermanno Pietrosemoli of Fundación Escuela Latinoamericano de Redes (EsLaRed), we were able to achieve a total of 6 Mbps bidirectional TCP throughput (3 Mbps each way simultaneously) over a single-hop 382 km WiLDNet link between Pico Aguila and Platillon in Venezuela. To the best of our knowledge, this is the longest distance at which a stable high-throughput WiFi link has been achieved without active amplification or custom antenna design. Each site used a 2.4 GHz 30-dBi reflector grid antenna with 5.3° beam-width and a 400 mW Ubiquiti SR2 radio card with the Atheros AR5213 chipset.

Figure 1 presents results from running WiLDNet on real links from our various deployments in Aravind (India), Ghana, Venezuela and our local Bay Area testbed. It verifies that we can match WiLDNet's performance over emulated links and greatly exceed the performance of the standard WiFi MAC protocol at long distances.

We find that we are no longer limited by performance

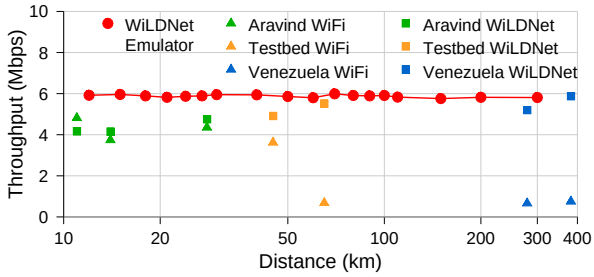

Figure 1: Comparison of TCP throughput for WiLDNet (squares) and standard WiFi MAC (triangles) from links in Aravind, Ghana, local testbed in Bay Area and Venezuela. Most urban links in Aravind had up to 5–10% loss, and so WiLDNet did not show substantial improvement over standard WiFi. However, WiLDNet's advantage increases with distance. Each measurement is for a TCP flow of 60s, 802.11b PHY, 11Mbps.

over long distances in rural networks. Instead, based on our experience in deploying and maintaining networks in the two rural regions of India for the last three years, we argue that operational challenges are the primary obstacle to successful deployments.

2.2 Challenges in Rural areas

Addressing these challenges requires looking at all levels of the system, from the power and base hardware, up through software and ease-of-use, all the way to training and remote management. The problems of reliable power, trained staff and access to equipment exist in developing regions in general, but are exacerbated in rural areas.

There are several specific reasons why maintenance in rural areas is hard.[1] First, local staff tend to start with limited knowledge about wireless networking and IT systems. This leads to limited diagnostic capabilities, inadvertent equipment misuse, and misconfiguration. Thus management tools need to help with diagnosis and must be educational in nature. Training helps as well, but high IT turnover limits the effectiveness, so education must be ongoing and part of the process.

Second, the chances of hardware failures are higher as a result of poor power quality and a harsh environment (e.g. lightning, heat, humidity, or dust). Although we do not have conclusive data about the failure rate of equipment for power reasons in rural areas, we have lost far more routers and adapters for power reasons in rural India than we have lost in our Bay Area testbed. This calls for a solution that provides stable, high-quality power to equipment in the field.

Third, many locations with wireless nodes, especially relays, are quite remote. It is important to avoid unnec-

[1]Note to reviewers: the issues and some Aravind data (but no AirJaldi data) appeared in our NSDR workshop paper [32].

essary visits to remote locations. Also, we should enable preventive maintenance during the visits that do occur. For example, gradual signal strength degradation could imply cable replacement or antenna realignment during a normal visit.

Fourth, the wireless deployment may often not be accessible remotely or through the Internet. The failure of a single link might make parts of network unreachable, even if the nodes themselves are functional. This makes it very hard for remote experts in another town or even local administrators to resolve or even diagnose the problem.

3 Background

Over the last two years we have deployed two rural wireless networks in India. One is at the Aravind Eye Hospital in south India where we link doctors at the centrally located Theni hospital to village clinics via point-to-point WiLD links. Patients video-conference over the links with the doctors for consultations. The other is in Dharamsala and is called the AirJaldi network. This network is primarily a mesh with a few long distance directional links that provides VOIP and Internet access to local organizations. Both networks have faced largely similar operational challenges, with some important differences. We describe these two networks in some detail below.

3.1 The Aravind Network

The Aravind network at Theni consists of five vision centers connected to the main hospital in Theni (Figure 2). The network has total of 11 wireless routers (6 endpoints, 5 relay nodes) and uses 9 point-to-point links. The links range from just 1 km (Theni - Vijerani) to 15 km (Vijerani - Andipatti). Six of the wireless nodes are installed on towers, heights of which range from 24–42 m; the others use short poles on rooftops or existing tall structures, such as the chimney of a paper factory. Recently, Aravind has expanded this model to their hospitals in Madurai and Tirunalveli where they have added two vision centers each using a total of five point-to-point links. The network is financially viable with a planned expansion to 50 clinics around 5 hospitals, which will provide access to eye care for 2.5M people.

Hardware: The wireless nodes are 266-MHz x86 single-board computers. They run a stripped-down version of Linux 2.4.26 stored on a 512 MB CF card. The routers can have up to 3 high-power Atheros 802.11 a/b/g radio cards (200mW). The longer links use 24dBi directional antennas. The routers consume about 4.5W when idle and 9.5W when transmitting at full bandwidth from 2 radios; 7W is the average power consumption for a node. We also run software for routing, logging and monitoring on the routers.

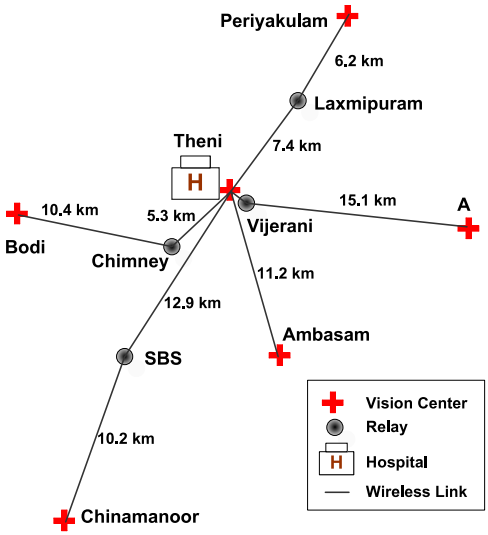

Figure 2: Aravind Telemedicine Network. Theni hospital is connected to 5 Vision Centers. The other nodes are all relays.

The routers are small and lightweight (less than 10 pounds), so we place them in water-proof enclosures and mount them near the antenna, typically on the same pole. This allows us to minimize the signal loss between the antenna and the radio. The routers are powered via power-over-ethernet (PoE), which allows a single cable from the ground to the router. We use uninterruptible power supplies (UPSs) to provide clean power, although we discuss solar power in Section 5.2.

Applications: The primary application is video conferencing and we currently use software from Marratech [17]. Although most conferences are doctor-patient, we also use it for remote training. We chose this software in part because it was easy for the staff to use. The typical throughputs on the links range between 5–7 Mbps with channel loss less than 2%. However, 256 Kbps in each direction is sufficient for very good quality videoconferencing. Our network is thus over-provisioned for the pilot phase. We also use the network to transmit diagnostic images taken with a digital camera that has been modified to connect to the slit lamp. There are also a range of standard e-mail and office applications. The hospital has a VSAT link to the Internet, but most of these applications only only intranet access within the network (except for remote management). Analysis of the traffic logs from last 12 months shows that each vision center has received 160 GB and transmitted 40 GB of mostly video traffic.

3.2 The AirJaldi Network

The AirJaldi network currently provides fast Internet access and VoIP telephony services to about 10,000 users at a radius of over 70 km in a rural mountainous terrain

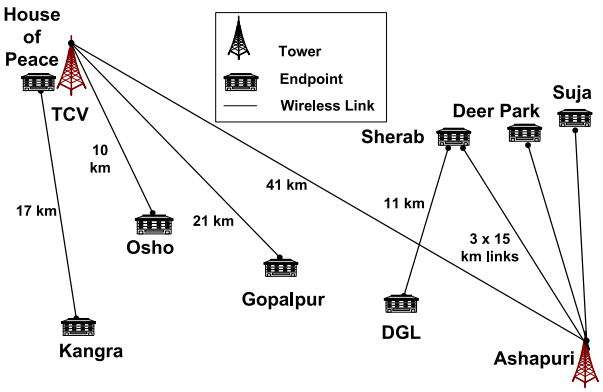

Figure 3: AirJaldi Network. There are 8 long-distance links with directional antennas with 10 endpoints.

characterized by extreme weather. The network has 8 long distance directional links ranging from 10 km to 41 km with 10 endpoints. In addition, the network also has over hundred low-cost modified consumer access points that use a wide array of outdoor antennas. Three of the nodes are solar-powered, relay stations at remote elevated places with climbable towers. All other antennas are installed on short (less than 5m) low-cost masts, typically water pipes, on the roof tops of subscribers.

Hardware: Most of the routers are extracted from consumer devices, either Linksys WRT54GL or units from Buffalo Technologies, and cost less than US$50. They are housed inside locally designed and built weatherproof enclosures, and are mounted next to the antennas in order to minimize signal loss over the otherwise longer RF cables. The antennas, power supplies and batteries are all manufactured locally in India. The router boards are built around a 200MHz MIPS processor with 16MB of RAM and 4MB of on-board flash memory with a low-power Broadcom 802.11b/g radio. We run a rudimentary Linux flavor called OpenWRT based on BusyBox. For long-distance links and major relay stations we also use slightly higher-end devices such as PCEngines WRAP boards, MikroTik routerboards and Ubiquiti LS2s with Atheros-based radios. The routers use open-source software for mesh routing, encryption, authentication, QoS, remote management and logging.

Applications: The Internet uplink of AirJaldi consists of 5 ADSL lines ranging from 144 Kbps to 2 Mbps to have a total of about 7 Mbps downlink and 1 Mbps uplink bandwidth. In the wireless network, the longest link from TCV to Ashapuri (41 km) achieves a throughput of about 4–5 Mbps at less than 2–5% packet loss, but the link from TCV to Gopalpur (21 km) only gets about 500–700 Kbps at 10–15% loss due to the absence of clear line of sight.

This bandwidth is sufficient for applications such as Internet access and VoIP that cater to the primary needs of the Tibetan community-in-exile surrounding Dharamsala, namely schools, hospitals, monasteries and other non-profit organizations. A cost-sharing model is used among all network subscribers to recover operational costs. The network is also now financially sustainable and growing fast. There are currently over 2200 unique MAC addresses on the network, which are mostly computers shared by a number of users daily. AirJaldi only provides connectivity to fixed installations that interconnect LANs of various organizations and does not offer wireless access to roaming users or mobile devices.

4 Operational Experiences

After having deployed these two wirleess networks at Aravind and AirJaldi over the last two years, we have experienced several operational challenges in both networks that have lead to significant downtimes, lower performance (e.g. increased packet loss), or increased maintenance costs. Any production network is difficult to maintain, but we argue that overcoming operational barriers in rural networks is particularly hard (Section 2.2).

Initially, we were involved in all aspects of planning, configuration, deployment, and maintenance of the networks with the specific end goal of ultimately transferring responsibility to our rural partners, primarily to ensure local buy-in and long-term operational sustainability. This process has not been easy. Our initial approach was to monitor these networks over the Internet and to provide support for local management, administering the network directly (bypassing the local staff) whenever required. But enabling remote management has been more challenging than expected because of severe connectivity problems. This aspect combined with the desire to enable local operational sustainability has led us to design the system with more emphasis on support for local management, a particularly challenging problem given limited local experience and challenging environments.

Although we were prepared to expect problems such as some connectivity issues, power outages, local misunderstandings of equipment usage, the actual extent of these problems has been very surprising, requiring a significant custom design of the management system. By aggregating the data logs of the incidents we have collected (and experienced) over the past few years, we first map these incidents to the three main reasons why the operational outages associated with those incidents were prolonged. Categorizing the faults in this manner is helpful because it disciplines us into thinking systematically about the faults. Thus, we first present the three main reasons, each of which is a combination of the challenges presented in Section 2.2.

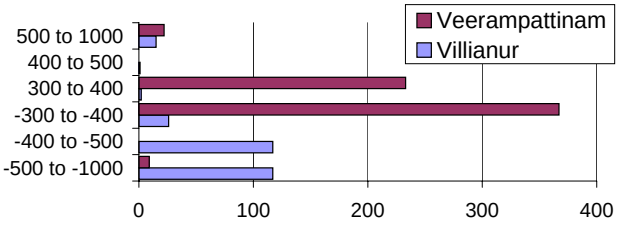

Figure 4: Histogram of power spikes from two rural villages. The bins (y axis) are the size range of the spike in volts, while the x axis is the count. Negative bins imply reversed polarity.

4.1 Components More Inclined to Fail

The operating conditions we have faced at Aravind and AirJaldi have actually contributed to decreased robustness of system components that would otherwise work quite reliably. The major culprit has been the lack of stable and quality power. Although issues such as frequent power outages in rural areas are well known, we were surprised by the *degree of power quality* problems in rural villages even when power is available. Before addressing the power issues (Section 5.2), not a single day went by without a failure related to low power quality in either network. Thus, any solution that focuses on system management must necessarily fix the power issues. Given the surprising quality of power problems in rural areas, which the larger networking community may not be aware of, and its significant impact on our network design, we take some time to document in detail our experience.

Low Power Quality: Figure 4 shows data on spikes from a power logger placed for 6 weeks in two different rural villages in southern India. We bin the spikes based on their size in volts; negative voltage means the polarity was reversed. We see many spikes above 500V, often with reversed polarity, and some even reaching 1000V! Clearly such spikes can damage equipment (burned power supplies), which has affected us greatly. We also see extended sags below 70V and swells above 350V (normal voltage in India is 240V). Although the off-the-shelf power supplies we use function well at a wide range of input voltages (80V–240V), they are not immune to surges and spikes. Also, locations that are far away from transformers are subject to more frequent and more extreme power fluctuations. Our first approach was to use UPS and battery backups. However, affordable UPS systems are only the "standby" type in that they are not really made to handle the range of power input reported above. Power flows through untouched if there is power at all; this has the effect of passing through the bad quality except during outages when the battery kicks in.

Failures from bad Power Quality: We have experienced a wide range of failures from such power quality issues. First, spikes and surges have damaged our power supplies and router boards. While in the AirJaldi network, we have lost at least 50 power supplies, about 30 ethernet ports and 5 boards to power surges, in the Aravind network, we have lost 4 boards, at least 5 power supplies and some ethernet ports as well.

Second, voltage sags have caused brown outs. Low voltages also leave routers in a wedged state, unable to boot up completely. The on-board hardware watchdog, whose job it is to reboot the router, can also be rendered useless suffering from the same low voltage situation, continuing to leave the router OS in a hung state. Third, fluctuating voltages cause frequent reboots, which damage the on-board flash memory through writes during reboot. However we have found out that because of the variability in the quality of power at different locations, the risk of damage to equipment such as corruption of flash disks also varies.

As a typical example, the router at SBS in Aravind rebooted at least 1700 times in a period of 12 months (Figure 5), roughly 5 times per day, going up to 10 times for some days. We contrast this with another router at Aravind deployed on top of chimney of a power plant from where it derives its power and which has uptimes going up to several months. Frequently fluctuating voltage prevents optimal charging of the battery backup and reduces its lifetime overall. In practice, we have observed that routers with more frequent reboots were more likely to get their flash disks corrupted over time. We had at least 3 cases of CF card corruptions at nodes co-located with the Vision Centers, shown in Figure 5, which experienced more reboots since staff at these locations shut down and boot up the routers everyday.

Lack of quality power increases not only down time but also maintenance costs. Traveling to remote relays just to reboot the node or replace the flash memory is expensive and sometimes has taken us several days, especially in Dharamsala where the terrain is very mountainous. In most power-related networking research, the goal has been to make more efficient use of available stable energy. This remains a goal for us too, whenever we have stable power.

Other Power-related Problems: Lightning strikes have damaged our radios. In Dharamsala in particular, which is one of the stormiest locations in India, and which has a mix of omni and directional antennas, we learned the hard way that most radios connected to omni antennas would get fried, while those connected to directional antennas commonly survive.

The explanation is that omnis are more attractive to lightning, as they are mounted on top of the mast and have a sharper tip, while directional antennas are typi-

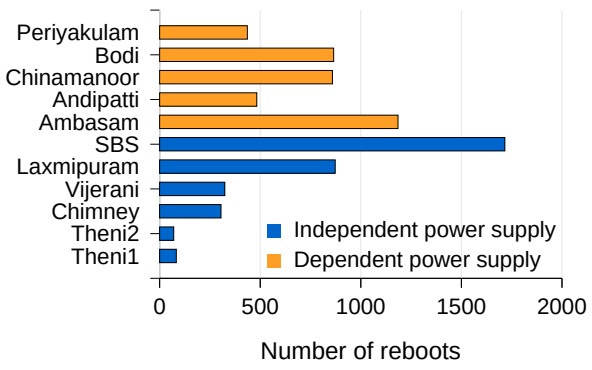

Figure 5: Number of reboots estimated per node in the Aravind network in about one year of operation. Nodes with dependent power supply are turned on or off with the vision center. Nodes with independent power supply are powered on independent of vision centers and they are typically relay nodes or hospital nodes.

cally mounted below the maximum height of the mast.

For reducing damage from lightning to omni antennas, we started to install them about 50cm below the top of the mast. This might however result in creating dead zones behind the mast where the signal from the antenna is blocked. To reduce this negative effect we sometimes use an arm to extend the omni antenna away from the mast hence reducing the dead-zone.

4.2 Fault Diagnosis is Difficult

Accurate diagnosis of the problem can greatly reduce response time and thus downtime. The most common description of a fault by our rural partners is that the "link is down". There are a wide variety of reasons for link outages and it is not always easy to diagnose the root cause. The lack of appropriate tools for inexperienced users combined with unreliable connectivity, which hinders detailed monitoring, prevents accurate diagnosis.

For example, a link may be down even if the remote node is up, but since the link is down, it is not possible to query the remote node for diagnosis. There have been many instances where rural staff have traveled to the remote site with great difficulty only to realize that it was a regular power shutdown from the grid or that it was a software problem which could have been fixed if there were an alternate backchannel to the router. Accurate diagnosis can save considerable time and effort, as well as prevent unnecessary travel. Furthermore, our own ability to help the local staff by logging in remotely to diagnose the problem is limited by connectivity. As an example, we used the VSAT link at Theni to login for monitoring and management purposes to aid local staff, but the VSAT backchannel has been up only 65% of the time.

And sometimes local misunderstandings of equipment usage make it even harder to diagnose problems. For example, as shown in Figure 6 an elevator shaft was constructed in front of the directional antenna at Aravind Theni, blocking it completely from the remote end. Whenever we were able to log into Theni, everything seemed fine except we could not communicate with the remote end. And we had no other access to the remote site. Local staff kept checking the remote end and did not (us included) think of checking the roof. The resulting downtime lasted for two months until we physically flew there and saw the problem!

Packet Loss due to Interference: At AirJaldi, in a remote village, decreased VoIP performance was reported for a particular link at very regular intervals. Without any additional information to diagnose the problem, no action could be taken and this behaviour persisted for three months. Finally, after some detailed monitoring by us (and not the rural staff), we saw a regular pattern of packet loss between 8am to 9am every day except Sundays. Scanning the channels showed no external WiFi interference. This information led us to find a poorly installed water pump that was acting a powerful spark generator, interfering with wireless signals in the vicinity. Without packet loss information, both the rural staff and ourselves would have trouble solving this one.

Signal Strength Decrease: In the Theni-Ambasam link in the Aravind network (Figure 2, we noticed a drop in signal strength of about 10 dB for about a month. Without further information it was hard to tell whether the antennas were misaligned, or the pigtail connectors were damaged, of the radio cards were no longer working well. In the end several different fixes over different trips were tried ranging from changing radio cards to connectors to antennas, and the signal strength bumped back up without it being clear what helped!

Network Partition: In many cases the network would be partitioned. For example, at Aravind, the rural operator misconfigured routing and added static routes while dynamic routing was already enabled. This created a routing loop partitioning the network. In another instance of operator error, the default gateway of one of the routers was misconfigured. There were also a few instances of operators changing the IP addresses of the endpoints of a link incorrectly, such that the link was non-functional even though it showed up as being associated. Finally, Figure 6 shows a hard-to-diagnose problem: hospital staff, unclear on the antenna concept, built an elevator shaft in front of the antenna, thus ending connectivity. This was not diagnosed until one of us flew to India, even though staff replaced the WiFi cards in the box.

"Fixing" by users: A recurring problem is that well-meaning rural staff try to fix problems through local

Figure 6: One example situation where the Theni to Vijerani link was completely obstructed by newly constructed elevator shaft. This problem was not resolved until we visited Theni after 2 months.

modifications when the root cause is not local. For example, at AirJaldi we have seen that when the upstream ISP suffers some downtime, rural staff tend to attempt to fix the problem thinking of it as a local problem. These local fixes typically create new problems, such as misconfiguration, and in a few cases have even resulted in damaged equipment. In these cases, local problems persist (now for a different reason) after the ISP resumes normal connectivity. Thus we need to develop mechanisms to indicate when the system is having remote problems, so as to prevent local attempts at repair.

The general theme is that no matter what the fault, if the link appears to be down with no additional information or connectivity into the wireless node, it is hard for even experienced administrators to get to the bottom of the problem. It is very difficult to distinguish between a power problems, board/cable failures, misconfigured wireless or IP settings, and a host of other potential causes.

4.3 Anticipating Faults is Hard

Node locations, especially relays, are quite remote. Site maintenance visits are expensive, time consuming, and require careful planning around the availability of staff, tools, and other spare equipment. Therefore, visits are generally scheduled well in advanced and are periodic, typically once every six months. In this scenario, it is especially important to be able to anticipate failures so that they can be addressed during the scheduled visits, or if catastrophic failure is expected, then a convincing case can be made for an unscheduled visit for timely action. But without an appropriate monitoring and reporting system, including backchannels, it is difficult to prepare for impending faults.

Battery Uptime: At both Aravind and AirJaldi we use battery backups. On loss of grid power when the battery starts discharging, the battery might last for an unknown amount of time after which the node will go down; typically rural staff has no idea when the battery will discharge. If this information is known, local staff can take corrective action by replacing the battery in time, preventing downtime of the network. Such feedback would also suggest if the problem is regional (as other routers will exhibit power loss too) or site-specific such as a circuit breaker trip.

Problem description	**System Aspects**
Component Failures	
Unreliable power supply	P
Bad power causing burnt boards and PoEs	P
CF card corruption: disk full errors	M, P
Omni antennas damaged by lightning	P, D
Fault Diagnosis	
Packet loss from interference	M
Decrease in signal strength	M
Network partitions	M, B
Self fixing by users	D
Routing misconfiguration by users	M, B, D
Failed remote upgrade	B, I
Remote reboot after router crash	B, I
Spyware, viruses eating bandwidth	M, D
Anticipating Faults is hard	
Finding battery uptime/status	M, B
Predict CF disk replacement	M

Table 1: List of some types of faults that we seen in both Aravind and AirJaldi. For each fault, we indicate which aspects of system design would help mitigate that fault. The different aspects are Monitoring (M), Power Design (P), Back Channel (B), Independent Control plane (I) and Network Design (D). The information on faults has been collated from logs and incident reports maintained by the local administrators and remote experts respectively.

Predicting Battery Lifetime: Battery life is also limited by the number of deep cycle operations permitted. Owing to the fluctuating voltages that do not charge the battery optimally, the lifetime of the battery degrades sharply from the reported lifetime. At Aravind, batteries rated with a lifetime of two years last for roughly three to six months. Information about the battery life can also enable prevention of catastrophic failures.

Predicting Disk Failure: We have observed that with frequent reboots over time, the disk partition used by us for storing logs accumulates bad *ext2* blocks. Unless we run *fsck* periodically to recover the bad blocks, the partition becomes completely unusable very soon. We have also seen that many flash disks show hardware errors, and it is important to replace the disk before they cause the router to completely fail.

5 System Architecture Design

Our goals are increased component robustness, ease of fault diagnosis, and support for predicting faults. To this end, we need to carefully consider 5 aspects of the system: Monitoring, Power, Backchannels, Independent Control Plane, and Network design. Table 1 indicates which aspects of the system design are important for reducing the impact of some the common faults presented in the previous section.

5.1 Monitoring

Monitoring is the most basic necessity for system management. It has been invaluable at Aravind and AirJaldi for faster response to problems.

During the initial deployment of Aravind, we faced two main challenges for designing a monitoring system. First, the Aravind network at Theni only allowed us to initiate connections from within the network. Second, the local staff were not familiar with Linux or with configuration of standard pull-based monitoring software such as Nagios [20].

This led us to build a *push-based* monitoring mechanism that we call "PhoneHome" in which each wireless router pushes status updates upstream to our US-based server. We chose this method over the general *pull-based* architecture in which a daemon running on a local server polls all the routers. The pull-based approach required constant maintenance via re-configuration of a local server every time a new router was added as the network expanded. The push-based approach however required only a one-time configuration per router during installation, which consisted of specifying the HTTP proxy (if needed).

The Aravind network has two remote connectivity options, both of which are slow and unreliable (Section 5.3): 1) a direct CDMA network connection on a laptop at the central hospital node, and 2) a VSAT connection to another hospital that has a DSL connection to the Internet. PhoneHome is installed on each of the wireless routers. All the routers periodically post various parameters to our US server website. Server-side daemons analyze this data and plot visual trends.

We collect node- and link-level information and end-to-end measurements. The comprehensive list of the measured parameters is given in Table 2. Most of these can be measured passively without interfering with normal network operation. However, several measurements, such as measuring the maximum throughput on a particular link, require active measurements. Some of these tests can be performed periodically (e.g. periodically pinging every host on the network), and some of them are done on demand (e.g. throughput achievable on a particular link at a given time).

We use PhoneHome mechanism to enable remote management as well. Every time PhoneHome connects to our server, it also opens reverse SSH tunnels back into the wireless node, which enables us to have interactive SSH access to the Aravind machines. As the VSAT connection only allows access over an HTTP proxy, we have to run SSH on top of HTTP, and configure PhoneHome with the proxy. In case of a direct connection to the Internet, no such configuration is required. Another option is to use OpenVPN on the routers that would open a VPN tunnel with a specified remote server.

Scope	Type	Measured Parameter
Node	Passive	CPU, disk and memory utilization, interrupts, voltage, temperature, reboot logs (number & cause), kernel messages, solar controller periodic data
	Active	disk sanity check
Link	Passive	*traffic:*, traffic volume(#bytes, packets) *wireless:* signal strength, noise level, # control packets, # retransmissions, # dropped packets *interference:* # of stations overheard & packet count from each, # corrupted packets
	Active	liveness, packet loss, maximum link bandwidth
System	Passive	route changes, pairwise traffic volume & type
	Active	pairwise end-to-end delay & max throughput

Table 2: Parameters collected by PhoneHome.

PhoneHome has helped with several operational issues. First, it maintains reachability information about the entire network, which has alerted local staff that the network is down and some action needs to be taken. Earlier, only a phone call from a rural clinic would alert the local administrator and depending on the inclination of staff at the rural clinic, this phone call would not always happen.

Second, kernel logs helped us diagnose some interesting problems. In certain instances, kernel logs showed that some routers had only one card active even though two cards were present. Following this bit of information, we figured out that low supplied power meant that both cards could not work simultaneously. In another instance, kernel logs and system messages allowed us to look at flash disk error messages and predict when disk partitions needed repartitioning or replacement.

Third, by posting the routing table and interface parameters, we were able to detect when routing was misconfigured, when IP addresses were incorrectly assigned and were able to inform the local staff of the error and provide them with helpful details.

Fourth, continuous monitoring of wireless link parameters helped us identify problems such as misalign-

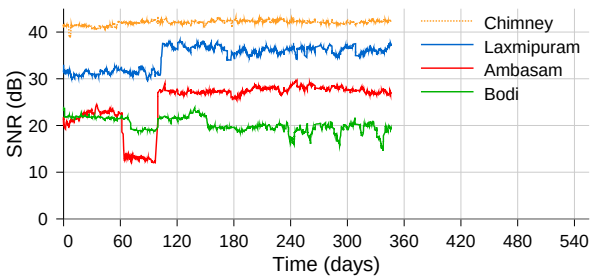

Figure 7: Signal strength (shown in dB) variation for all links. Each point is average of measurement over 2 days. The Ambasam link shows a temporary drop in SNR of 10 dB for about 40 days. While the Bodi link is gradually degrading as it's SNR has dropped by 4 dB over the last year, the Chimney link's SNR has remained constant.

ments of directional antennas. Figure 7 shows the signal strength variation in time, for all the network links. Although for the majority of links the signal strength is fairly constant, some links show variation over time. For example, link between Ambasam to Theni experienced a 10 dB drop which was then fixed (after considerable time) by rural staff to finally result in an increase of about 25 dB. Also, the Bodi link is showing a steady decline in signal strength, which most likely indicates degradation of the connector or cable.

Tradeoffs: We contrast this with monitoring at AirJaldi. In Dharamsala, we use various off-the-shelf tools such as Nagios, SmokePing to collect node, link, and network level parameters.

Information is stored at a local data server in Dharamsala and then copied to a US server for detailed analysis. Various graphing toolkits such as MRTG [22] are used to visualize trends and detect anomalies. The difference in approach compared to Aravind is in part due to the slightly higher level of experience of staff at AirJaldi and in part due to the better connectivity we have to AirJaldi. The advantage of having local servers that poll for information is that they can be configured by local staff to look for relevant problems, but this is only advantageous when local staff have gained some experience.

After two years of operation, the local Aravind staff, some of whom we lost due to turnover after getting more experience through our training, are somewhat more familiar with configuration and now show less apprehension in taking the initiative to maintain their own. Therefore, we are now starting to use a *pull-based* model. In general, while starting out, it is better to use minimal configuration *push-based* mechanisms for data collection, until there is enough local expertise to move to a more flexible *pull-based* approach.

5.2 Power

Power quality and availability has been our biggest concern at both Aravind and AirJaldi. Low-quality power damages the networking equipment (boards and power adaptors) and sometimes also batteries. Over 90% of the incidents we have experienced have been related to low power quality. Thus, designing to increase component reliability in the face of bad power is the most important task. We have developed two separate approaches to address the effects of low power quality. The first is a Low Voltage Disconnect (LVD) solution, which prevents both routers from getting wedged at low voltages and also over-discharge of batteries. The second is a low-cost power controller that supplies stable power to the equipment by combining input from grid and battery. In many cases, we prefer to avoid the grid completely and just use solar because of grid power fluctuations.

Low Voltage Disconnect (LVD): Over-discharge of batteries can reduce their lifetime significantly. Owing to the poor quality of grid power, all AirJaldi routers are on battery backup. LVD circuits, built into battery chargers, prevent over-discharge of batteries by disconnecting the load (router) when the battery voltage drops below a threshold. As a beneficial side-effect, they prevent the router from being powered by a low-voltage source, which may cause it to hang. Off-the-shelf LVDs oscillated frequently, bringing the load up and down, and eventually damaging the board and flash memory. Every week, there were roughly fifty reboot incidents per router due to hangs caused by low voltage. However, we designed a new LVD circuit with no oscillation and since then the hangs per week per router have reduced to near zero in the Dharamsala network.

Power Controller: We have developed a microcontroller-based power controller. The first version is a solar power controller with smart battery management, while the second one, still under development, supports grid or solar power.

Overall, the board combines three tasks into one board: providing quality 12 V to the nodes, managing the charging and discharging of the battery, and enabling solar. The combination is novel for its price of about US$70. We use TVS diodes to absorb spikes and surges and a robust voltage regulator to get clean 12V power from wide ranging input conditions. We have not lost any boards powered by the controller, but we only have eight months of experience with the board so far. Besides price, the controller has several other novel features: power-over-ethernet, peak-power tracking, temperature sensing, and support for remote monitoring and management.

Figure 8 shows the flow of current through the board over a 60-hour period. First, we note that power is always available to the router. When enough sunlight is

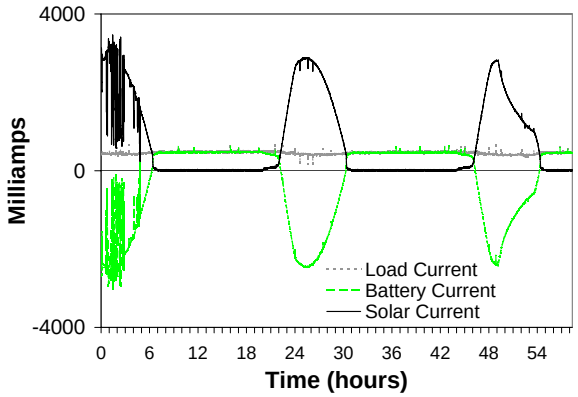

Figure 8: Current flow over 60 hours. The load stays even at 7W, while the solar panel and battery shift their relative generation over time. The battery current is negative when it is charging.

available, the solar panel powers the router and charges the battery. During periods of no sun, the battery takes over powering the router. The frequent swings observed on the left part of the graph are typical for a cloudy day. The graphs also demonstrate how the battery is continually charged when sunlight is available.

The controller is trivial to use: just connect the batteries and the solar panels and then connect to the wireless node using just a single ethernet cable, which carries the power and enables remote management. The controller enables remote management by reporting loads, battery levels, and solar panel parameters. So far, we have primarily been using this information for remote diagnosis of power and router issues.

Tradeoffs: The real cost of power in rural areas is not just the raw grid electricity costs, but the cost of overcoming power availability and quality issues through battery-backups, chargers, and solar panels. These costs can be quite high and therefore, we choose to use the solar only for relays which are so remote that it makes sense to pay the higher costs for cleaner power and features such as remote management (through the controller). At less remote and critical sites, we tend to use "dumb" analog chargers to reduce costs.

5.3 Backchannels

A wide variety of problems at Aravind and AirJaldi have caused link downtimes, leaving remote nodes disconnected. The failure of a single link makes part of the network unreachable although the nodes themselves might be functional. In many cases, if we had alternate access to the nodes, the fixes were simple such as correcting a router misconfiguration, or rebooting the router remotely. It is important to have out-of-band access or a backchannel to the nodes that is separate from the primary wireless path to it. Backchannel access is also useful in cases of complex failures where the battery is discharging but the router is already down for other reasons. Information about the battery status over the backchannel would still be helpful. We have tried several approaches to backchannels at both networks.

Network Backchannel: At the Aravind Theni hospital, we already had some form of backchannel into the Theni network through V-SAT. We use PhoneHome to open an SSH tunnel over the V-SAT link through an HTTP proxy at the Aravind Madurai hospital. We configure PhoneHome to post monitoring data to our US-based server every 3 hours and also to open a reverse SSH tunnel through which we can log back in for administration purposes. However, the V-SAT link was flaky. Out of the 2300 posts expected from the router at Theni over 143 days (2 posts every 3 days), we only received 1510 of them, or about 65% of them. So this particular backchannel was not very reliable in practice, sometimes not working for long stretches of time. As a result, we used the solitary hospital laptop to connect directly to the Internet using a 1xRTT CDMA card to improve the availability of a backchannel into the network. However, this laptop was used for several other purposes (shared hardware is a common feature in rural areas) and was mostly unavaible. Furthermore, in many instances network backchannel was not enough as the local wireless network would itself be partitioned.

Node Backchannel: At AirJaldi, we built a node backchannel mechanism using GPRS connectivity. In India at the moment, GPRS connectivity costs roughly $10 per month for unlimited duration and bandwidth. We used a Netgear WGT634U router, interfaced through its USB 2.0 port with a mobile phone. The router runs PPP over GPRS and sets up an OpenVPN tunnel to a remote server. To enable remote diagnosis using this link, the backchannel router is connected to the main wireless router using ethernet and optional serial consoles. The backchannel router can also power-cycle the wireless router using a solid-state relay connected to one of its GPIO pins.

This approach has two advantages. First, the cellphone network is completely independent of the wireless link. Second, even though the mobile phone is charged from the same power source, it has its own battery which allowed access via GPRS even if the main power source was down. We had additional battery backup for the Netgear router. However, the additional router with battery backup did add additional maintenance complexity. One approach to simplify this setup for console access would be to use a linux GPRS phone but we have not tried it yet.

Tradeoffs: Our experience with the GPRS backchannel in terms of providing real utility for system manage-

ment has been mixed. Many common problems can be solved by alternative means in simpler way. In cases of incorrect configuration of routers, we can imagine using the GPRS backchannel to fix problems. But at Aravind, when misconfigurations rendered routing useless, we used cascaded hop-by-hop logins to move through the network, although this depended on at least the endpoint IP addresses to be set correctly. However, we can also use Link Local IP addressing [27] to have independent hop-by-hop backchannels. Each link gets a local automatic IP addresses from a pre-assigned subnet that would work even when the system wide routing does not work. This can also be implemented by using virtual interfaces in the Atheros wireless driver [4]. Such virtual link configuration approaches could be permanent and also independent of any network configuration

We have also used the built-in WiFi radio of the backchannel netgear router to remotely scan local air interfaces for interferences or low RF signals from other routers, particularly after storms in Dharamsala. But we found the *most useful* feature of the GPRS backchannel to be console access to the router in case of failed attempts at remote firmware upgrades. But arguably, good practices of testing the upgrade locally on an idential router may suffice. This would mean reducing the router platforms used in the field to standardize testing. However, this can be hard to do practically, especially in initial phases as rural networks move from pilots to scale. In future work we intend to continue exploring the idea of cellphone backchannels.

One idea is that instead of using GPRS as the backchannel, a cheaper mechanism could be using SMS channels. With SMS, console access would need to be implemented from scratch. Instead of console access, one approach would be to just query the remote router over SMS. The reply would have power parameters (grid power, remaining battery, voltage level of power supply), and basic status information from the wireless board if it is up. The phone would be connected to the router within the enclosure over serial. This is often feasible because many places have more ready access to SMS compared to GPRS. For example, all our rural clinics at Aravind, have some degree of SMS coverage provided by 2-3 providers at least.

5.4 Independent Control Mechanisms

Independent or failure independent mechanisms are essential for managing systems remotely. The best solution is to have fully redundant systems, but they are often too expensive. An intermediate solution, more viable for rural areas is to have some independent modules that enable diagnosis and some recovery (but not full functionality and so cannot do complete failover).

Alternate backchannels can enable independent access to various system components, and we include them in the design of independent control mechanisms. However in situations where the main router itself is wedged or is in a non-responsive state, we need to use independent components that can reset or reboot the main router. In this section, we discuss independent software control and independent hardware control.

Software watchdog: Essential software services can enter bad states and crash. For instance, wireless drivers have entered bad states that prevent the wireless card from receiving or transmitting packets even though the OS still keeps running. It is essential to have a monitoring service that can either restart software services on the router or reboot the router itself.

We have built a software watchdog which is run by `cron` every 4 minutes. A configuration file lists what parameters to monitor such as IP reachability to a set of hosts, channel, SSID and BSSID changes, wireless operation mode as well as a list of processes that need to be running on the node. The configuration file also lists what actions to take upon failure of any of the tests, and how often a test is allowed to fail before an action is taken. Actions taken range from bringing the wireless interface down and up again, unloading and reloading kernel modules, and rebooting the system. We are using this software watchdog in the AirJaldi network currently.

Hardware watchdog: An on-board hardware watchdog will reboot the router periodically unless it gets reset periodically after receiving keep-alive messages from the router. This is a vital feature, but most of the routers used in AirJaldi do not actually have on-board watchdogs. To address this we have designed for $0.25, a simple external hardware watchdog (a simple delay circuit) that interfaces with the board's GPIO line. We have designed this watchdog to plug into the router's power input port and to also accept PoE-enabled power so it can also power PoE-less routers, which allows us to use lower-cost routers as well. All the boards we use at Aravind have on-board watchdogs, but if board is wedged due to lower supply, then the watchdog itself will be rendered useless. However, we can avoid this by using the LVDs we have designed. In some cases, we are also using the power controller described in Section 5.2 as a form of external hardware watchdog where it monitors the board over ethernet (also PoE) and power-cycles it if it does not hear a keep alive in time.

Enabling Safe Fallback: We can use the backchannel and the independent control plane to implement *safe fallback mechanism* for upgrades. When upgrading the OS on a wireless router, we could use a software watchdog that will be configured to check that the upgrade does not violate any required properties. For example, the board should be able to initialize all the drivers, and ping local

interfaces and remote nodes as well. If these are not satisfied, we should go back to a previously known fail-safe OS state. This can be combined with a hardware watchdog mechanism that can reboot the router to a fail-safe OS state in cases where the newly installed OS does not even boot. This is future work for us.

5.5 Network Design

As mentioned in Section 2, our first step in designing rural wireless networks to implement the WiLDNet MAC protocol to achieve high throughputs on long distance point-to-point links.

However, we it is not always possible design a network with just point-to-point links. For example in topologies where there is not much angular separation between clients from a central location, it is infeasible to have separate point-to-point links to each client using directional antennas. In those cases, an interesting compromise is to use sector antennas where some nodes run a point-to-multipoint (PMP) MAC protocol to provide access to a large number of clients that do not have very high individual throughout requirements while the long distance links still use the point-to-point MAC protocol [9]. We are currently in the process of extending the WiLDNet MAC protocol to support point-to-multipoint configurations as well.

In addition to the above issues with protocol design, we have had to rethink the design of several other aspects of our network ranging like OS software and diagnostic tools for local staff so that it easier to manage and more robust to failures.

Read-only Operating System: We saw from experience in the Aravind network that the CF cards used in the wireless routers would often get corrupted because of frequent and unexpected reboots.

Sometimes writing a single bit of data can corrupt the flash. We discovered in the AirJaldi network that if an oscillating LVD keeps rebooting a router, any CF write during boot-up will finally fail and corrupt the flash. Unfortunately most boot loaders write to flash during the boot up process. We had replace the boot-loaders with our own version that does not perform any writes at all.

In addition, we found out that it is better to mount the main OS partition read-only so that no write operations occur throughout the normal life cycle of the router. For collecting logs, we have one read-write partition. However, in production systems, it would be preferable to have all the partitions to be read-only mounted.

Configuration and Status Tools: To train local staff in administration of wireless network without exposing them to details of underlying Linux configuration files, we designed a web based GUI for easy configuration and display of simple status information about a particular router.

However to further aid local staff in diagnosing problems we need to build tools that can query the network and present an easy to understand picture of the problem. For example, if run from a PC at a vision center, it can indicate that the local wireless router is up and running but reachability to the remote router is down. This will minimize the *self-fixing* problem where local staff unnecessarily try to modify local installations without waiting for the network to come back up.

6 Related Work

WiFi-based deployments: There have been several development projects that use WiFi-based network connectivity for applications such as healthcare (Ashwini [3]), the Digital Gangetic Plains [12]), e-literacy and vocational training (the Akshaya network [2]), education (CRCNet [11]) and so on. However, our deployment is possibly the first that takes a systematic approach toward availabilty and both projects are in active use by thousands of users. There are a number of community wireless projects in the US ([8, 21, 5]) that use a combination of open source monitoring tools, but they focus on smaller range of operational challenges. Raman et al. in [26] try to summarize all the open issues in deploying rural wireless such as network planning, protocols, management, power and applications but they mainly focus on the modifying the MAC and conserving power using *Wake-on-LAN* [19] techniques.

Long distance WiFi: Given the cost and performance promises of 802.11 rural connectivity, there have been several efforts to analyze the behavior [30, 10] and improve the performance of multi-hop long-distance WiFi networks, including the design of an TDMA-based MAC layer [25] that relies on burst synchronization to avoid interference, and channel allocation policies to maximize network throughput [24]. Our work [23] builds and improves on these efforts, delivering a real-world implementation that delivers high-performance (5-7Mbps for links up to 382 Km), predictable behavior, and flexibility to best accommodate various types of traffic. Raman *et al.* [29] also investigate network planning solutions that minimize costs by optimizing across the space of possible network topologies, tower height assignments, antenna types and alignment and power assignments.

Remote management: There has been a lot of work on remote operation and upgrades to large scale datacenters [7, 1] that have reliable power and network connectivity. On the other extreme, there has been work on online software upgrades to sensor networks as well [16]. However remote management solutions for wireless networks that could possibly located in remote rural regions has not received a lot of attention. In this spectrum, Mer-

Type of problem	Instances	Recovery time	Who solved it	Who should have solved it
Circuit breaker trip at node locations	S:26 V:33 C:4	1 day	**Staff**: Flip the breaker physically at location, added UPS	**Staff**: Monitoring system should trigger that node is down
PoE stopped working (transformer explosion)	1	1-7 days	**Integrators**: Replaced PoE	**Staff**: Replace PoE by checking connectivity and components
Loose ethernet cable jacks	M:12 C:2 T:7	1-7 days	**Experts**, **Staff**: Re-crimp RJ-45 with help from experts, train staff to check for loose cables	**Staff**: Monitoring system should trigger that wireless link is up but ethernet is down
Routing misconfiguration: incorrect static routes, absent default gateway	Routing:2 Gateway:4	1-7 days	**Experts**: Using reverse SSH tunnel **Integrators**: Using config tool	**Staff**/**Integrators**: Use config tool for routing
CF card corruption: disk full errors	Replace:2 Fix:10		**Integrators**, **Staff**: Replace CF card **Experts**: Run fsck regularly	**Automatic**: Run fsck on problem **Staff**: Replace CF cards after config.
Wall erected in front of antenna: link went down	1	2 months	**Experts**: After physical verification	**Staff**: Ensure line of sight
Ethernet port on board stopped working	M:2	N/A	**Integrators**: Replace router board	**Staff**/**Integrators**: Replace boards

Table 3: List of failures that have occurred since January 2005 at various locations in the Aravind network. For each fault, we indicate who among **staff**, **integrators**, or remote **experts** solved the problem. This information has been collated from logs and incident reports maintained by the local administrators and remote experts respectively. It is an underestimate as all failures are not accounted for in the local logs maintained by local staff.

aki [18] provides a remote management suite for WiFi networks where all the monitoring, configuring, diagnosis and periodic updates for their field-deployed routers is hosted of the Meraki server.

7 Conclusion

We presented a wide range of operational challenges from two years of deployment experience with two different rural wireless networks. Although work to date has largely been on performance, the primary obstacle to real impact for these networks is keeping them alive over the long term. We conclude by summarizing some of the broad lessons of these deployments, which we believe apply to other projects in developing regions.

Prepare for absence of local expertise: Most projects assume that training will solve the need for local IT staff, but this is quite difficult. Although we have had some success with this at AirJaldi, it is limited due to high staff turnover. In some sense, better training leads to higher turnover. Instead, we have worked to reduce the need for highly trained staff on multiple levels.

Starting at the lowest layers, we have pushed hard on improving the quality of power and the ability of nodes to reboot themselves into a known good state. We have added substantial software for self validation (again with reboots) and for data collection and monitoring. We also developed support for remote management, although it is limited by connectivity issues, especially during faults; in turn, we looked at backchannels to improve the reach for remote management. We also developed GUI tools that are much easier for local staff to use and that are intended to be educational in nature.

At the highest level, we met these challenges by creating a three-tier management hierarchy, in which local IT vendors (called *Integrators*) with expertise in installing rural wireless networks were hired to form a mid-level of support between local staff and ourselves. Over time, the rural staff has learned to handle more issues, the IT vendors handle some issues (such as installing new links), and we handle fewer issues. This is shown in the partial list of failures in Table 3 from the Aravind network. Here we indicate for each fault, both how it was solved and how long it took in the initial phase, and also how it should be solved once the we successfully migrate the management of the network to be more local.

Redesign of components is often enough: As mentioned earlier in Section 4, that because of harsh environmental conditions and flaky power, commodity components fail more often in rural areas. One solution is to use expensive equipment such as military grade routers and big battery backups or diesel generators, as is done with cellular base stations at great cost. However, we aim to use low-cost commodity hardware for affordability.

In practice, even simple redesign of selected hardware components can significantly decrease the failure rates without adding much cost. In addition to getting WiFi to work for long distances, we also developed software and hardware changes for low-voltage disconnect, for cleaner power, and for more reliable automatic reboots, and we developed better techniques to avoid damage due

to lightning and power surges.

The real cost of power is in cleaning it up: The key is to understand that the real cost of power in rural areas, is not the cost of grid power supply, but of cleaning it using power controllers, batteries and solar-power backup solutions. Some development projects incorrectly view the cost of electricity as zero, since it is relatively common to steal electricity in rural India.[2] However, the grid cost is irrelevant for IT projects, which generally need clean power (unlike lighting or heating). Due to short lifetimes of batteries and UPSs, power cleaning is a recurring cost. Solar power, although still expensive, is thus more competitive than expected as it produces clean power directly. We currently use solar power for relays or other locations where power is not available, and try to manage grid power elsewhere. At the same time, it is critical improve the tolerance for bad power of all of the equipment, and to plan for sufficient back up power.

In the end, there remains much to do to make these networks easier to manage by the local staff; progress is required on all fronts. However, even the changes implemented so far have greatly reduced the number of failed components (mostly due to lightning and bad power), have increased the ability of local staff to manage network problems, and have helped to grow the networks without significantly growing the staff. Both networks are not only helping thousands of real users, but are also experiencing real growth and increased impact over time.

References

[1] S. Ajmani, B. Liskov, and L. Shrira. Scheduling and simulation: How to upgrade distributed systems. In *HotOS-IX*, 2003.

[2] Akshaya E-Literacy Project. *http://www.akshaya.net*.

[3] Ashwini: Association for Health Welfare in the Nilgiris. *http://www.ashwini.org*.

[4] Atheros. MadWiFi driver for Atheros Chipsets. *http://sourceforge.net/projects/madwifi/*.

[5] Bay Area Research Wireless Network. *http://www.barwn.org*.

[6] P. Bhagwat, B. Raman, and D. Sanghi. Turning 802.11 Inside-out. *ACM SIGCOMM CCR*, 2004.

[7] E. Brewer. Lessons from Giant-scale Services. *IEEE Internet Computing*, 2001.

[8] Champaign-Urbana Community Wireless Network. *http://www.cuwin.net*.

[9] K. Chebrolu and B. Raman. FRACTEL: A Fresh Perspective on (Rural) Mesh Networks. *ACM Sigcomm Workshop on Networked Systems for Developing Regions (NSDR)*, August 2007.

[10] K. Chebrolu, B. Raman, and S. Sen. Long-Distance 802.11b Links: Performance Measurements and Experience. In *ACM MOBICOM*, 2006.

[2]The tolerance of theft is a kind of subsidy for the poor, but it is badly targeted as others steal power too. India loses about 42% of its generated electricity to a combination of theft and transmission losses (vs. 5–10% in the US) [14].

[11] CRCNet: Connecting Rural Communities Using WiFi. *http://www.crc.net.nz*.

[12] Digital Gangetic Plains. *http://www.iitk.ac.in/mladgp/*.

[13] Drishtee Dot Com Limited. The Drishtee Project. *http://www.drishtee.com*.

[14] M. Gregory. India Struggles with Power Theft. *BBC News Online*, May 2006. http://news.bbc.co.uk/2/hi/business/4802248.stm.

[15] ITC Limited. The e-Choupal Initiative. *http://www.echoupals.com*.

[16] P. Levis, N. Patel, D. Culler, and S. Shenker. Trickle: A Self Regulating Algorithm for Code Propagation and Maintenance in Wireless Sensor Networks. *NSDI*, 2004.

[17] Marratech. Videoconferencing Software. *http://www.marratech.com*.

[18] Meraki. Meraki Wireless Mesh Routers. *http://www.meraki.net*.

[19] N. Mishra, K. Chebrolu, B. Raman, and A. Pathak. Wake-on-WLAN. In *Proceedings of WWW 2006*, May 2006.

[20] Nagios. Wireless Monitoring. *http://www.nagios.org*.

[21] NY Wireless Network. *www.nycwireless.net*.

[22] T. Oetiker. MRTG: The Multi Router Traffic Grapher. *http://oss.oetiker.ch/mrtg/*.

[23] R. Patra, S. Nedevschi, S. Surana, A. Sheth, L. Subramanian, and E. Brewer. WiLDNet: Design and Implementation of High Performance WiFi Based Long Distance Networks. *NSDI*, 2007.

[24] B. Raman. Channel Allocation in 802.11-based Mesh Networks. In *IEEE INFOCOM*, Apr. 2006.

[25] B. Raman and K. Chebrolu. Design and Evaluation of a new MAC Protocol for Long-Distance 802.11 Mesh Networks. In *ACM MOBICOM*, Aug. 2005.

[26] B. Raman and K. Chebrolu. Experiences in using WiFi for Rural Internet in India. *IEEE Communications Magazine*, Jan. 2007.

[27] RFC 3927: Dynamic Configuration of IPv4 Link-Local Addresses . *http://www.ietf.org/rfc/rfc3927.txt*.

[28] D. D. Savigny, H. Kasale, C. Mbuya, and G. Reid. *Fixing Health Systems: Linking Research, Development, Systems, and Partnerships*. International Development Research Centre, 2004. ISBN: 1552501558, http://www.idrc.ca/tehip.

[29] Sayandeep Sen and Bhaskaran Raman. Long Distance Wireless Mesh Network Planning: Problem Formulation and Solution. *WWW*, 2007.

[30] A. Sheth, S. Nedevschi, R. Patra, S. Surana, L. Subramanian, and E. Brewer. Packet Loss Characterization in WiFi-based Long Distance Networks. *IEEE INFOCOM*, 2007.

[31] L. Subramanian, S. Surana, R. Patra, M. Ho, A. Sheth, and E. Brewer. Rethinking Wireless for the Developing World. *Hotnets-V*, 2006.

[32] S. Surana, R. Patra, and E. Brewer. Simplifying Fault Diagnosis in Locally Managed Rural WiFi Networks. *ACM Sigcomm Workshop on Networked Systems for Developing Regions (NSDR)*, August 2007.