WIRELESS MULTIHOP NETWORKS IN MISSION CRITICAL REALTIME MONITORING AND ALERTS FOR CONSTRUCTION SITES

Winston K.G. Seah
Institute for Infocomm Research, Singapore
winston@i2r.a-star.edu.sg

G.H. Tan
SysEng (S) Pte Ltd, Singapore
syseng@singnet.com.sg

Abstract

In major construction projects involving extensive excavation and tunneling, it is crucial to have accurate realtime monitoring to ensure that support structures are not excessively stressed as these could lead to collapse and fatalities. The integration of machine-to-machine (M2M) technologies has been proposed to improve the process of transferring data from the sensors in the monitoring sites to be promptly processed into information that can assist engineers in handling unexpected events. While the use of M2M technologies in the construction industry has been increasing, much more can be exploited from wireless communications to improve the productivity levels and more importantly the safety aspects. In this paper, we present a realtime monitoring and alert system integrated with a multihop wireless network. Besides replacing the wiring which can pose significant problems in a construction site, wireless communications also makes the system less vulnerable to lightning and other problems. With the wireless transmission devices located near the sensors, we reduce the wiring substantially and using a multihop architecture enables us to extend the communication range by relaying data from one radio to another until the on-site data logger.

INTRODUCTION

In major construction projects involving extensive excavation and tunneling, it is crucial to have accurate realtime monitoring to ensure that support structures are not excessively stressed as these could lead to collapse and fatalities. The integration of machine-to-machine (M2M) technologies has been proposed to improve the process of transferring data from the sensors in the monitoring sites to be promptly processed into information that can assist engineers in handling unexpected events [1]. While the use of M2M technologies in the construction industry has been increasing, much more can be exploited from wireless communications to improve the productivity levels and more importantly the safety aspects. In this paper, we present a realtime monitoring and alert system integrated with a multihop wireless network. Besides replacing the wiring which can pose significant problems in a construction site, wireless communications also makes the system less vulnerable to lightning and other problems. With the wireless transmission devices located near the sensors, we reduce the wiring substantially and using a multihop architecture enables us to extend the communication range by relaying data from one radio to another until the on-site data logger. As transmission between radios is short range, we also save power and extend the lifetime of the power source. This network uses commercial-off-the-shelf wireless technology like WiFi [2] and Zigbee [4] making deployment relatively simple. Yet another benefit can be derived – noise that can be easily picked up by the wires and cause false alerts [5] will be reduced, and to further reduce the probability of errors, intelligence can be built into the on-site data logger to initiate additional readings from the sensor in question and also other sensors in the locality. In fact, most embedded WiFi and Zigbee devices have sufficient onboard computing power to make this decision to initiate the additional readings and/or perform some simple local decisions to change the frequency of sensor readings to suit the on-site conditions.

STATE-OF-THE-ART AND TECHNOLOGY ISSUES

Construction site monitoring involves a set of processes and procedures that measure physical attributes, e.g., beam pressure, water pressure and temperature. These attributes are monitored in a scheduled manner by sensors and transmitted via wires to an on-site gateway, and subsequently to a central server via the General Packet Radio System (GPRS). At the central server, the data is processed and presented in suitable formats to the engineers and other decision makers who can access this information anytime anywhere via the Internet. In the event of any anomaly, the inspection team will be alerted immediately [1]. Another approach connects groups of sensors to WiFi access points that are installed at various locations within the construction site. An engineer then moves around and uses a notebook or portable device with a WiFi interface to collect data via these WiFi access points [3]. While the above-mentioned use of GPRS has enabled realtime availability of critical data with minimal human intervention, the use of wires to connect the sensors to the on-site gateway is very costly, non-recyclable

and also susceptible to damage by the construction workers. These contribute to the high cost of site monitoring as: (i) the expensive wires cannot be re-used on new construction sites; and (ii) the high occurrence of accidental cutting by the construction workers incurs delays and additional overheads to repair and replace.

Due to physical constraints such as water, muddy terrains and deep troughs, there are certain areas in the sites where wires simply cannot be laid. The current solution is manual monitoring involving a trained worker with a probe to measure the attributes on-site. Manual monitoring is susceptible to human error when the workers record down the identification strings that indexes the location and the attributes. These strings of numbers and mixed-case alphabets contribute to the high incidences of errors. The recorded data will then be consolidated at the on-site office where another person will update a central database for monitoring. Such a scenario is ideal for an automated monitoring solution using wireless communications.

Benefits of Wireless Communications

The high costs of laying wires lie in the material and labour costs, which translates to sunken costs that cannot be recovered. Wires are also susceptible to lightning strikes in which high voltages of electricity can travel along the wires and destroy the connected devices, like the data loggers and gateway. Usage of wireless communications based on off-the-shelf technologies like WiFi and Zigbee can provide a cost effective solution that is reusable, from one site to another. Moreover, a wireless solution expands deployment coverage and can be extended to areas that previously cannot be connected via wires. Reducing the amount of wires on site also reduces the impact of lightning problems.

State of Multihop Wireless Communications Technology

While there is a vast amount of work and published literature on wireless communications, they tend to focus on the technical aspects and benefits of each available wireless technology rather than how these technologies can be applied in a real life context, in this case, realtime structural monitoring. Majority of the research have also been conducted through simulations, and do not consider non-ideal scenarios such as random interference, terrain conditions and background noises. Consequently, the deployment results are expected to deviate from the simulation results; there exists a gap between research and application, which needs to be bridged. Besides GPRS and the traditional WiFi, wireless multihop networks is emerging as a good candidate for construction site monitoring. One of its benefits includes extending the range of a network without having to incur high fixed-infrastructure costs. Kuladinithi, *et al*. [6] discuss the potential of mobile ad-hoc communications in the architectural, engineering and construction (AEC) industry and propose the use of the Ad-hoc On-Demand Distance Vector (AODV) [7] routing protocol due to its reactive nature and lower overheads as compared to proactive protocols such as the Optimized Link State Routing (OLSR) protocol [8]. The lower traffic overheads of the AODV protocol also saves energy and extends the lifetime of the devices.

WiFi and Mesh Networking

WIFI, which is based on the IEEE 802.11 standard, has been criticized for its poor performance in mesh networks which originates from its handshaking mechanism for reducing collisions. Studies have also shown that wireless multihop networks using shortest-path routing protocols exhibit poor throughput performance due to the possibly weak signal quality of links that packets are transmitted over. Furthermore, IEEE 802.11 mesh networks tend to consume large amounts of energy due to overhearing of packets intended for other destinations. The energy usage increases linearly with the number of nodes in the network when all the nodes are in a linear/string topology. Other factors that affect the energy consumption include idle listening on the channel, and unsuccessful transmissions arising from interference and collisions. Despite the criticisms of the IEEE802.11 protocol in an ad-hoc mesh network scenario, the widespread proliferation of WiFi routers (due to their cheap cost and off-the-shelf availability) running the OLSR and AODV protocols based on OpenWRT [10] show that such a solution is still practical.

MULTIHOP WIRELESS NETWORK FOR REALTIME MONITORING

The current state-of-the-art Real Time Monitoring system used in Singapore [5] uses sensors welded onto metal beams in excavation sites which are then hard-wired to multiplexers and data loggers, with wires stretching hundreds of metres from sensors to the data loggers. The data loggers scan the sensor readings and transmit the sensor data via GPRS to a central server automatically every 10 minutes. The system automatically processed and calibrated each sensor when the data is received. If the sensor reading exceed its software preset limits, SMS alerts are automatically sent to assigned users within 10 minutes, so that user can have early warning to perform site checks to prevent disasters.

The multihop wireless network approach aims to improve performance, lower costs and extend coverage by replacing the long wires that are costly to lay, susceptible to noise and false alerts, and vulnerable to accidental damage leading to work interruption and further costs. It also enables locations which previously could not be connected via wires and require manual data collection and monitoring, to be included in the automated monitoring system. Instead of connecting all the sensors via long cables to the data loggers, groups of sensors will be connected to multiplexers that are linked by a WiFi-based multihop network to the data logger; multiplexers are placed near the sensors to keep the cables as short as possible. Multiple data loggers can also be deployed in a large site and linked via this mesh network to an on-site computer. The proposed wireless multihop network is shown in Figure 1.

The current deployment scenario that we have used to test our system is the construction sites of the Singapore Mass Rapid Transit system. The excavation sites for the subway tunnel are supported by metal beams which are constantly monitored to ensure that they are not subjected to excessive stress that may lead to structural failure and collapse. The network comprises five WiFi routing nodes in a linear string topology with a distance of about 100m between nodes. Data from up to 200 sensors can be multiplexed onto each node, giving a data rate of up to 2 kilobytes(KB) every 10 minutes.

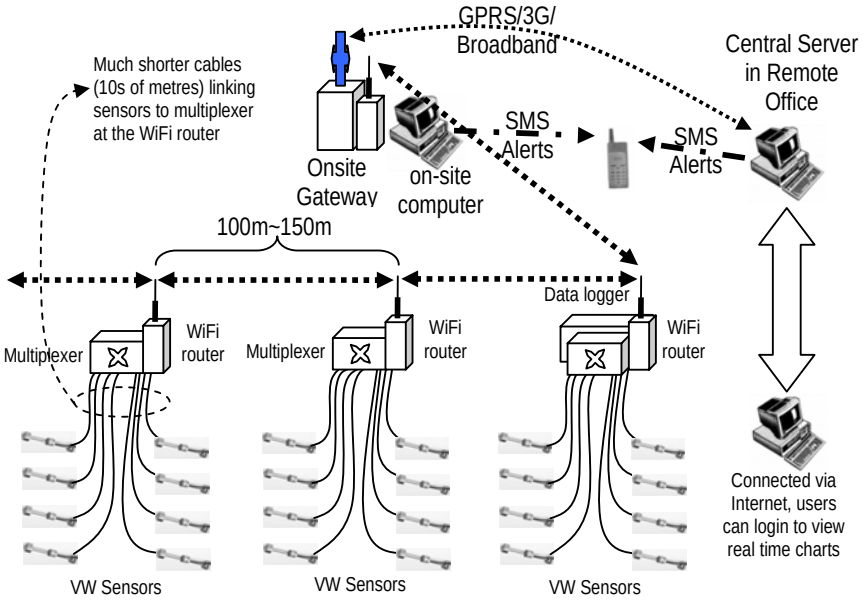

Figure 1. Wireless Multihop Network for Realtime Monitoring

Routing Node Implementation

While there are many off-the-shelf WiFi solutions available in the marketplace that range from full fledged industrial products to commercial home and office solutions, they are designed to support applications like web browsing, not realtime telemetry and monitoring applications. Our objective is to find a low cost, yet robust solution to replace the wires in the automated monitoring process and we have selected the Linksys WRT54G routers for this purpose. To use commercial off-the-shelf routers to form a multihop network, the proprietary firmware must be replaced with a customized firmware that allows us to load and run our own codes. This series of network devices are the most widely supported in the open source community, including OpenWRT. To enable multihop communication, the nodes are required to run ad hoc routing protocols. While there are many ad hoc routing protocols available, only three protocols have been implemented on OpenWRT: two implementations of AODV and one of OLSR. Since our devices are powered by solar panels in the day and then run on industrial batteries through the night, energy efficiency is a critical factor which makes AODV a better candidate [6]. Furthermore, as AODV is a reactive routing protocol, it can cater for the case whereby handheld devices carried by the construction workers enter the multihop network to perform ad hoc manual readings. We therefore selected the AODV implementation on OpenWRT by Uppsala University [11] which has been tested by the open source community and shown to be more robust.

Performance Benchmarking and Tuning

Before we can deploy the multihop network, we have to understand the hardware performance of the selected routers, especially in terms of their range. The ability to know and control the range of our hardware is important for us to deploy our multihop topology accurately. It has been reported in an online review [12] that the range of Linksys WRT54G router is 76 feet in an office environment. However, these measurements are valid only for the 54 Mbps Wireless-G operating mode and there is a lack of study on the range of different operating rates and transmission powers. Hence, we conducted preliminary experiments (setup as shown in Figure 2) to determine the range that the device can achieve using different transmission rates (54Mbps, 11Mbps and 2Mbps) and transmission power levels (84mW, 79mW, 42mW and 1mW).

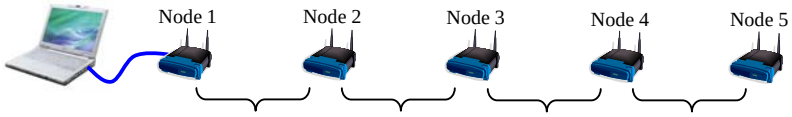

Figure 2. Performance Tuning Network Setup

After determining the range of the routers, we investigated the performance of the AODV protocol. Using logfiles of previously collected data from an operational system, 2Kbyte blocks of data are transmitted every 10 minutes from nodes 2, 3, 4 and 5, to node 1 which emulates the gateway node. Prior to sending each 2KB, AODV performs a route discovery and setup since the previous route has expired [7]. As we are dealing with mission-critical data, we use a reliable (TCP-based) data-transfer protocol to send the data packets. Two transmission power levels, 79mW and 42mW, were used with nodes placed 100m apart (similar to the actual deployment scenario) and operating at 11Mbps transmission rate:

- 79mW – This value allows us to study the performance of the AODV protocol with the nodes operating at the default settings. However, due to the higher transmission power, packets bypass intermediate nodes enroute to node 1.
- 42mW – This value, as ascertained in the earlier tests, ensures a multihop topology when the nodes are 100m apart. E.g., when node 5 sends data to node 1, packets will pass sequentially through each intermediate node without bypassing any of them.

We evaluate two key performance metrics, namely, the *packet delivery ratio* (PDR), and the *average end-to-end delay*. The PDR, as shown in Figure 4, is the percentage of packets successfully delivered to the gateway (Node 1), while the average end-to-end delay, as shown in Figure 3, is the time taken by packets to reach the gateway including the time taken by AODV to setup the route from the sending node to the gateway.

In Figure 4, we note that the Packet Delivery Ratio (PDR) is better when a higher transmission power of 79mW as compared to 42mW. Transmitting at 79mW, nodes 2 and 3 are able to send all their packets to the gateway, and trace files reveal that packets from node 3 are usually sent directly to the gateway, bypassing node 2. As the distance to the gateway increases, there is a need to route the packets via intermediate nodes and

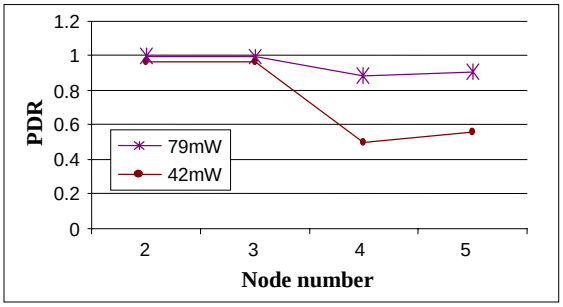

Figure 4. Performance Tuning - PDR

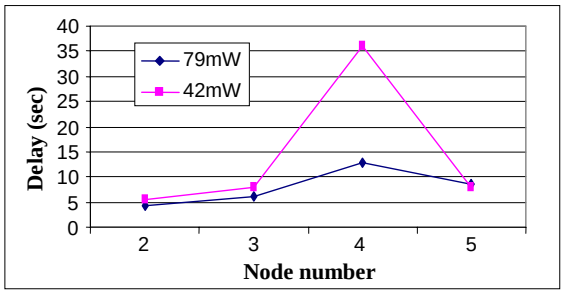

Figure 3. Performance Tuning - Delay

therefore contend for the shared wireless bandwidth which consequently lead to packet loss due to interference and collisions. If the AODV route discovery and setup process fails, the corresponding data packet will be discarded and considered lost. Node 4's poor performance is due to its position that requires it to compete with nodes 3 and 5. Although node 3 also has two other nodes competing for access, its packets can reach the gateway in one hop, unlike node 4's packets which need to be further relayed. When 42mW is used, all the nodes can only reach its immediate next hop and nodes that are further away naturally experience poorer PDR. Node 4's disadvantage is also more evident in this scenario. Transmitting at higher power consumes more energy which is undesirable in our context. In Figure 3, we show the average end-to-end delay. A performance trend that is similar to the PDF is observed. Due to the traffic contention experienced by node 4, there are more packet retransmissions that result in greater delay and higher energy consumption.

Scheduling for Better Performance

Considering that the transmission rate used by the nodes is 11Mbps, the data traffic from the monitoring process is very low at 2KB per 10 minutes, which should not cause any contention at all. However, such contention does occur and can be attributed to the case when all the nodes try to transmit their 2KB data blocks at about the same time. Upon analyzing the transmission log files across all the nodes, we have observed that the poor performance is due to channel congestion and the inability to establish

routes to the gateway (node 1) within the timeout period of the high level data-transfer protocol. Thus, deployment of pure off-the-shelf WiFi routers running AODV protocol does not quite meet the requirements for delivery of mission critical data.

Scheduling the transmission of data packets has been shown to be effective in preventing congestion in wireless multihop networks [13]. In our system, we implement a simple application layer scheduling algorithm while leaving the hardware, firmware and AODV routing protocol unmodified. Our algorithm schedules the transmission times of each node such that no other nodes within the two-hop topology will transmit at the same time. E.g. if node 5 is transmitting, then nodes 3 and 4 must not transmit, in order to prevent the hidden terminal problem. While the hidden terminal problem is addressed by the IEEE802.11 protocol's Request-to-send(RTS)/Clear-to-send(CTS) procedure, the Route Request (RREQ) messages used by AODV to setup a route are broadcast in the network and does not invoke the RTS/CTS procedure. If the route setup is unsuccessful due to contention and collision of RREQ messages, the data packets will be discarded since there is no route available to send them.

We define ***t*** as the scheduled interval/slot for a node to send its 2KB data block, and a *cycle* as the duration covering all the nodes' time slots, as shown in Figure 5. We tested a set of different values for ***t***, ranging from 3 seconds to 15 seconds. From earlier trials, it has been observed that the average time required by a node to send its data to the gateway takes between 3 and 8 seconds, depending on how far it is from the gateway. Using ***t*** values in this range aims to test for the maximum data rate that the network can support while ***t*** values more than 8 seconds serve to benchmark an unloaded network.

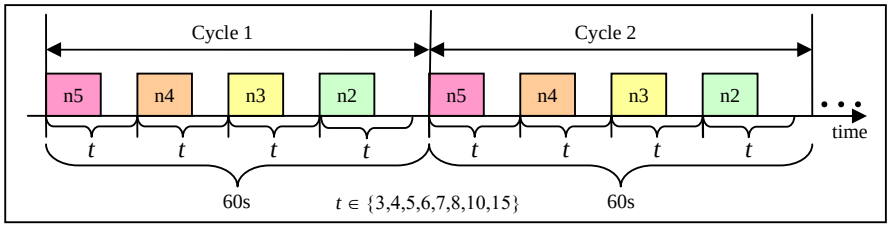

Figure 5. Transmission Scheduling

We repeated the experiments with the scheduling algorithms implemented in the nodes and, as expected, the best performance occurs when ***t*** = 8 seconds, where the PDR for the four nodes are optimal at more than 0.97 at both 79mW and 42mW, and the minimum average end-to-end delay to transfer the 2KB data block is 5 seconds. The highest data rate achieved is 0.25KB/s or 150KB/10mins which is sufficient for the construction site's requirements of 2KB/10mins.

ONSITE DEPLOYMENT AND FIELD TESTS

The wireless multihop network was then deployed in an actual tunnel excavation site for field testing. Due to site regulations and restrictions, we were unable to deploy the same network setup as our earlier experiments. The deployment site has a length of about 300m, and as such, we can either put three nodes, 100m apart or place five nodes,

60m apart. We chose to deploy five nodes, 60m apart in this case as we felt that the obstructions in and around the area will very likely reduce the transmission range and we might not be able to establish the sufficiently stable wireless links if they are 100m apart. This is especially true for some nodes which had to be deployed in narrow walkways and were surrounded by metal structures. The tests were carried out using the same set of parameter values as before.

An immediate observation was that despite the shorter distance between nodes, transmitting at 42mW was barely able to maintain the links between adjacent nodes resulting constant route disruptions. This invoked remedial action by AODV and added more network traffic in the form of Route Error (RERR) messages. When nodes operated at 79mW transmission power, with scheduling of data packets, the PDR was greater than 0.72 in most cases (as shown in Figure 6; $t = 0$ refers to no scheduling). The poor performance of node 3 was caused by its location which was in a low lying area with many metal obstructions. The presence more abundant metal beams adversely affected the performance of all the nodes, not just node 3. This is also clear from the end-to-end delay performance shown in Figure 7. With the higher transmission power, nodes' transmission ranges fluctuate frequently, causing route disruptions which invoke AODV remedial procedures. Moreover, there is no optimal scheduling interval.

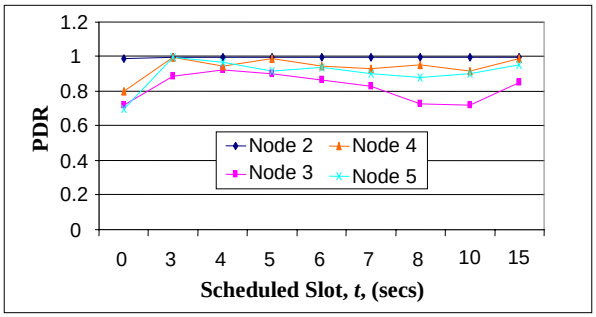

Figure 6. Onsite Field Test Performance - PDR

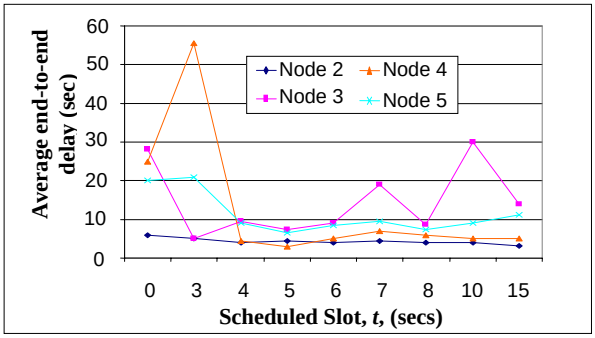

Figure 7. Onsite Field Test Performance - Delay

SUMMARY AND FUTURE WORK

Realtime monitoring of critical structures in construction sites can benefit from the adoption of wireless communications technologies, bringing about error reduction and cost savings. There are many existing technologies available off the shelves which can be utilized for this purpose. In this paper, we studied the feasibility of a wireless multihop network built from available off-the-shelf firmware, WiFi devices and open-source protocols to replace costly cabling used in current realtime monitoring systems. We propose a simple scheduling algorithm that enhances the data delivery performance and validate it through experiments and on-site field tests. For our ongoing and future work, we will be conducting more extensive tests to understand the channel conditions in typical construction sites and design algorithms that are optimized to meet the stringent requirements of mission-critical realtime construction site monitoring.

References

1. Tan, G.H., Ng, T.G. and Brownjohn, J., 'Real Time Monitoring and Alert Systems for Civil Engineering Applications Using Machine-to-Machine Technologies', Proc. of the Int'l Conf on Structural and Foundation Failures, Singapore, Aug 2004.
2. WiFi Alliance [http://www.wi-fi.org].
3. Ludwig, C. and Constable, E., 'Wireless Tiltmeters Monitor Stability during Trench Excavation for Reno Transportation Rail Access Corridor', Geotechnical News (Dec 2005) 29-32.
4. Legg, G., 'Zigbee: Wireless Technology for Low Powered Wireless Sensor Networks', TechOnLine, May 6 (2004) [http://www.techonline.com].
5. Tan, G.H., *et al*., 'Real Time Monitoring and Alert in Excavation Works using Machine-to-Machine Technologies', Proc. of the 2nd Int'l Conf on Structural Health Monitoring of Intelligent Infrastructure (SHMII-2), Shenzhen, China, Nov 2005.
6. Kuladinithi, K., Timm-Giel, A. and Görg C. Mobile Ad-hoc Communications in AEC Industry, ITcon 9 (2004) 313-323.
7. Perkins, C.E., Belding-Royer, E.M. and Das, S., 'Ad Hoc On-Demand Distance Vector Routing (AODV)', IETF RFC 3561, Jul 2003.
8. Clausen, T. and Jacquet, P., 'Optimized Link State Routing Protocol (OLSR)', IETF RFC 3626, Oct 2003.
9. De Couto, D.S.J., Aguayo, D., Chambers, B.A. and Morris, R., 'Performance of multihop wireless networks: Shortest path is not enough', ACM SIGCOMM Computer Communication Review 33 (1) (2003) 83-88.
10. OpenWRT – Linux distribution for embedded devices (2006) [http://openwrt.org/].
11. Uppsala University, AODV-UU implementation version 0.9.1, (2006) [http://core.it.uu.se/core/index.php/AODV-UU]
12. Knorr, E., 'Linksys Wireless-G Broadband Router WRT54G', CNET.com, Feb 28 (2003).
13. Huang, Y., Gong, W. and Towsley, D., 'Application layer relays for wireless 802.11 mesh networks', Proc of the 2nd IEEE Workshop on Wireless Mesh Networks (WiMesh), Reston, VA, U.S.A. Sep 25, 2006.